



GFI Product Manual

GFI EventsManagerTM
User Manual



<http://www.gfi.com>

info@gfi.com

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

All product and company names herein may be trademarks of their respective owners.

GFI EventsManager is copyright of GFI SOFTWARE Ltd. - 1999-2011 GFI Software Ltd. All rights reserved.

Document Version: ESM-UM-EN 03.00.00

Last updated: December 5, 2011

Contents

1	Introduction	1
1.1	About this manual	1
1.2	Conventions used in this manual	2
1.3	About GFI EventsManager	2
1.4	Key Features	3
1.5	How does GFI EventsManager work?	6
1.6	Navigating the GFI EventsManager management console	8
2	Getting Started	9
2.1	Introduction	9
2.2	What is a computer log?	9
2.3	What are Windows Event Logs?	9
2.4	What are W3C logs?	10
2.5	What are Syslogs?	10
2.6	What are SNMP Traps?	11
2.7	What are SQL Server audit logs?	11
2.8	What are Oracle Server audit logs?	11
3	Installation	12
3.1	Introduction	12
3.2	Where can I install GFI EventsManager on my network?	12
3.3	System requirements	15
3.4	Upgrading from a previous version	17
3.5	Firewalls and Anti-virus software	17
3.6	Computer identification considerations	17
3.7	Installation procedure	18
3.8	Running GFI EventsManager for the first time	20
4	Event browsing	27
4.1	Introduction	27
4.2	Navigating the Events Browser	27
4.3	Creating custom Root Views / Views	28
4.4	Event color-coding options	31
4.5	Event finder tool	32
4.6	Export to CSV tool	33
4.7	Rule finder tool	33
4.8	Reporting options	34
4.9	Switching database	35
5	Reporting	36
5.1	Introduction	36
5.2	Navigating the Reports tab	36
5.3	Available reports	37
5.4	Managing reports	38
5.5	Generating reports	40
5.6	Analyzing reports	41
5.7	Creating custom reports	41
5.8	Daily Digest	52

5.9	Settings report	53
5.10	Rules report	54
5.11	Operational history	56
5.12	Activity overview	57
6	Manage event sources	61
6.1	Introduction	61
6.2	Managing event sources groups	61
6.3	Adding event sources.....	64
6.4	Configuring event source properties	66
6.5	Microsoft SQL Server sources.....	72
6.6	Oracle Server sources	77
6.7	GFI LanGuard event sources.....	85
6.8	GFI EndPointSecurity event sources.....	86
7	Using event processing rules	89
7.1	Introduction	89
7.2	Collecting Windows events	91
7.3	Collecting Text logs	93
7.4	Collecting Syslogs	95
7.5	Collecting SNMP Traps	98
7.6	Collecting custom events	102
7.7	Triggering a manual event source scan.....	104
8	Manage rule-sets	105
8.1	Introduction	105
8.2	Adding a rule-set folder.....	106
8.3	Creating new events processing rules.....	106
8.4	Creating a new rule from an existing event	111
8.5	Advanced event filtering parameters	112
9	Customizing alerts and actions	114
9.1	Introduction	114
9.2	Configuring Default Classification Actions	115
9.3	Configuring Alerting Options	116
10	Configuring users and groups	123
10.1	Introduction	123
10.2	Managing user accounts.....	123
10.3	Managing groups	128
10.4	Managing Console Security and Audit Options	130
10.5	Managing Database and Files Backend security	134
11	Status monitoring	135
11.1	Introduction	135
11.2	General status view	135
11.3	Job activity view.....	138
11.4	Statistics view	139
12	Database Operations	141
12.1	Introduction	141

12.2	Why database maintenance?	141
12.3	Creating a new database backend.....	142
12.4	Configuring Database Operations.....	144
12.5	Creating maintenance jobs	145
12.6	Editing existing maintenance jobs.....	155
13	Miscellaneous	158
13.1	Enabling permissions on event sources manually	158
13.2	Enabling permissions on event sources automatically	170
13.3	Disabling UAC to scan event sources	175
13.4	Command line tools	175
13.5	Auto updating GFI EventsManager	181
13.6	Product licensing.....	182
13.7	Version information	183
14	Troubleshooting	185
14.1	Introduction	185
14.2	Common issues	185
14.3	Knowledge Base	188
14.4	Web Forum.....	188
14.5	Request technical support.....	188
14.6	Build notifications	189
15	Glossary	191
	Index	195

List of tables

Table 1 - Key features	3
Table 2 - GFI EventsManager engines	7
Table 3 - Devices supported by GFI EventsManager	13
Table 4 - Benefits of installing GFI EventsManager in DMZ	14
Table 5 - Hardware requirements	15
Table 6 - Software requirements: Operating system	15
Table 7 - Software requirements: Other components	15
Table 8 - System requirements: Event source settings	15
Table 9 - System requirements: Ports and protocols	16
Table 10 - System requirements: Firewall permissions	16
Table 11 - Quick Launch Console options	25
Table 12 - Navigating the Events Browser	27
Table 13 - Event Browser: Create new view	28
Table 14 - Event Browser: Create new report	35
Table 15 - Navigating the Reporting tab	36
Table 16 - Available reports	37
Table 17 - Managing reports	38
Table 18 - Create folder: Schedule options	39
Table 19 - Analyzing reports tools	41
Table 20 - Create Report dialog: General options	43
Table 21 - Create Report dialog: Chart options	45
Table 22 - Create Report dialog: Schedule options	46
Table 23 - Defining restrictions: Field Operators	49
Table 24 - Defining restrictions: Query Condition tools	50
Table 25 - Add Column Definition options	52
Table 26 - Settings report heading information	53
Table 27 - Rules report heading information	55
Table 28 - Operational history reports	56
Table 29 - Export operational history options	57
Table 30 - Activity overview headings	57
Table 31 - Export operational history options	59
Table 32 - Event source group options	62
Table 33 - Synchronization properties - General tab	63
Table 34 - Example of synchronizations	63
Table 35 - Event sources: Audit policy options	69
Table 36 - Auditing options	70
Table 37 - Microsoft SQL Database group: General tab	72
Table 38 - Microsoft SQL Database group: Logon Credentials	72
Table 39 - Microsoft SQL Database group -SQL Server Audit	73
Table 40 - Microsoft SQL Database group - Settings	73
Table 41 - Microsoft SQL Database - General tab options	75
Table 42 - Microsoft SQL Database - Connection Settings tab	76
Table 43 - Microsoft SQL Database - Settings tab options	77
Table 44 - Oracle Server supported audits	77
Table 45 - Oracle Server configuration stages	78
Table 46 - Oracle Database group - General tab	79
Table 47 - Oracle Database group - Oracle Audit	79
Table 48 - Oracle Database - General tab options	81
Table 49 - Oracle Database - General tab options	82
Table 50 - Oracle Database - Audit by Objects	83
Table 51 - Oracle Database - Audit by Statements	84
Table 52 - Windows Event Logs collected by GFI EventsManager	91
Table 53 - Configuring Windows Event Log processing	92
Table 54 - Configuring W3C processing	94
Table 55 - Configuring Syslog processing	96
Table 56 - Configuring SNMP Traps processing	100
Table 57 - Events Processing Rules	105
Table 58 - Rule-set folders available in GFI EventsManager	105
Table 59 - Configuring new events processing rules: Actions	110
Table 60 - Create rule from event dialog options	112
Table 61 - Parameters available in the Event ID field	112
Table 62 - Parameters available in the Source, Category and User fields	113
Table 63 - Parameters available in the Message and Process fields	113

Table 64 - Alerting methods	114
Table 65 - Supported alerting actions	114
Table 66 - Alerting Options dialog: Email	117
Table 67 - Alerting Options dialog: SMS	119
Table 68 - Alerting Options dialog: SNMP	120
Table 69 - Alerting Options dialog: General	120
Table 70 - Status monitoring: General view	136
Table 71 - Status monitoring: Job activity view	138
Table 72 - Status monitoring: Statistics view	139
Table 73 - Available database operations	141
Table 74 - Configuring database operations	144
Table 75 - Database operations: Schedule options	147
Table 76 - Database operations: Schedule options	149
Table 77 - Table 78 - Database operations: Export file name structure	149
Table 79 - Database operations: Schedule options	151
Table 80 - Database operations: Schedule options	153
Table 81 - Database operations: Schedule options	155
Table 82 - Database operations: Schedule options	157
Table 83 - CMD tools	175
Table 84 - CMD: ESMCmdConfig.exe functions	176
Table 85 - CMD: Esmdlbm.exe functions	178
Table 86 - Auto update options	182
Table 87 - Terms used in this manual	191

List of screenshots

Screenshot 1 - The GFI EventsManager management console	8
Screenshot 2 - Pre-requisite check	18
Screenshot 3 - Customer and License detail screen	19
Screenshot 4 - Logon information screen	19
Screenshot 5 - Quick Start Dialog	21
Screenshot 6 - Events processed from local machine	22
Screenshot 7 - Select the type of event source	23
Screenshot 8 - Select computers from result	23
Screenshot 9 - Process events from selected machines	24
Screenshot 10 - GFI EventsManager Quick Launch Console	25
Screenshot 11 - Events Browser	27
Screenshot 12- Custom view builder	29
Screenshot 13- Edit view restriction	29
Screenshot 14- Customize View tab	30
Screenshot 15 - Sample: New Root Views and Views	30
Screenshot 16 - Color coding configuration	31
Screenshot 17 - Advanced Color Filter	32
Screenshot 18 - Event finder tool	32
Screenshot 19 - Export events tool	33
Screenshot 20 - Find rule	34
Screenshot 21 - Report from view button	34
Screenshot 22 - Switch database dialog	35
Screenshot 23 - Navigating the Reporting UI	36
Screenshot 24 - Create Report Folder dialog	38
Screenshot 25 - Generating a report	40
Screenshot 26 - Report sample	40
Screenshot 27 - Preview Report: Analyzing	41
Screenshot 28 - Creating a new report	42
Screenshot 29 - Creating a report: General	43
Screenshot 30 - Creating a report: Layout	44
Screenshot 31 - Createing a report: Chart	45
Screenshot 32 - Createing a report: Schedule	46
Screenshot 33 - Createing a report: Options	47
Screenshot 34 - Creating a report: Adding conditions	48
Screenshot 35 - Creating a report: Edit Query Conditions	49
Screenshot 36 - Customizing the condition	50
Screenshot 37 - Define custom column conditions	51
Screenshot 38 - Daily Digest email settings	52
Screenshot 39 - Daily digest emai	53
Screenshot 40 - Generate configuration report	54
Screenshot 41 - Settings report sample	54
Screenshot 42 - Generate configuration report	56
Screenshot 43 - Operational history report	57
Screenshot 44 - Operational history dialog	57
Screenshot 45 - Operational history report sample	57
Screenshot 46 - Activity overview : Export button	58
Screenshot 47 - Activity overview dialog	58
Screenshot 48 - Activity overview report sample	59
Screenshot 49 - Add new event source group	62
Screenshot 50 - Synchronization properties - General tab	63
Screenshot 51 - Synchronization properties -Schedule tab	64
Screenshot 52 - Add new event source wizard	65
Screenshot 53 - Browse the network for connected computers	65
Screenshot 54 - Event sources properties dialog	67
Screenshot 55 - Configuring alternative logon credentials	68
Screenshot 56 - Specify operational time	69
Screenshot 57 - Event source properties: Audit tab	70
Screenshot 58 - Event-processing configuration tabs	71
Screenshot 59 - Database Servers Groups	72
Screenshot 60 - Microsoft SQL Database group - SQL Server Audit tab	73
Screenshot 61 - Add new Microsoft SQL server	74
Screenshot 62 - Microsoft SQL Database properties: General tab	75
Screenshot 63 - Microsoft SQL Database properties: Connection Settings tab	76

Screenshot 64 - Microsoft SQL Database properties: Settings tab	77
Screenshot 65 - Database Servers Groups	78
Screenshot 66 - Oracle Database group - General tab	78
Screenshot 67 - Oracle Database group - Oracle Audit tab	79
Screenshot 68 - Add new Oracle server	80
Screenshot 69 - Oracle Database - General tab	81
Screenshot 70 - Oracle Database - Connection Settings tab	82
Screenshot 71 - Oracle Database -Audit by objects tab	83
Screenshot 72 - Oracle Database -Audit by statements tab	84
Screenshot 73 - Event generated by GFI LanGuard	85
Screenshot 74 - Event generated by GFI EndPointSecurity	87
Screenshot 75 - Rule-sets folder and Rule-sets	89
Screenshot 76 - Log processing, classification and actions flowchart	91
Screenshot 77 - Computer group properties: Configuring Windows Event Logs parameters	92
Screenshot 78 - Selecting the events to be collected	93
Screenshot 79 - Computer group properties: Configuring W3C event processing parameters	94
Screenshot 80 - Computer group properties: Syslog processing parameters	96
Screenshot 81 - Configuring Syslog Servercommunication port	97
Screenshot 82- Syslog server options	98
Screenshot 83 - Computer group properties: SNMP processing parameters	100
Screenshot 84 - Configuring SNMP Traps	101
Screenshot 85- SNMP Traps options	101
Screenshot 86 - Custom event logs setup	102
Screenshot 87 - Custom event logs dialog	103
Screenshot 88 - Configure file storage dialog	104
Screenshot 89 - To create new rules, rich-click a rule-set and select Create new rule...	107
Screenshot 90 - Create new events processing rule: Select the logs which the rule will be applied to	107
Screenshot 91 - Create new events processing rule: Configure the rule conditions	108
Screenshot 92 - Create new events processing rule: Select the event occurrence and importance	109
Screenshot 93 - Create new events processing rule: Select the action	110
Screenshot 94 - Creating a rule from an event	111
Screenshot 95 - New rule from event dialog	112
Screenshot 96 - Configuring default classification actions	115
Screenshot 97 - Default Classification Actions dialog	115
Screenshot 98 - Configuring Alerting Options	116
Screenshot 99 - Configuring Email options	117
Screenshot 100 - Configuring Network alerts	118
Screenshot 101 - Configuring Network alerts: Format message dialog	118
Screenshot 102 - Configuring SMS alerts	119
Screenshot 103 - Configuring SNMP alerts	120
Screenshot 104 - Configuring User settings	124
Screenshot 105 - EventsManager Administrator properties	124
Screenshot 106 - Configuring the typical working hours of an alert recipient	125
Screenshot 107 - Selecting alerts to be sent during and outside working hours	125
Screenshot 108 - Notification groups to which a user belongs	126
Screenshot 109 - Configuring GFI EventsManager administrator privileges	127
Screenshot 110 - GFI EventsManager new user privileges	128
Screenshot 111 - New groups setup	129
Screenshot 112 - Select Security Options to enable the log-in system	130
Screenshot 113 - Login window	131
Screenshot 114 - Anonymization options	132
Screenshot 115 - Audit Options	133
Screenshot 116 - Auto-discovery credentials	134
Screenshot 117 - Dashboard View Options	135
Screenshot 118 - GFI EventsManager Status: General view	135
Screenshot 119 - GFI EventsManager Status: Job Activity view	138
Screenshot 120 - GFI EventsManager Status: Statistics view	139
Screenshot 121 - Archive Storage Folder dialog	143
Screenshot 122 - Database Operations Options dialog	144
Screenshot 123 - Creating a new Database Operation	145
Screenshot 124 - Import from File	146
Screenshot 125 - Import from file: Decrypt	146
Screenshot 126 - Creating a new Database Operation	147
Screenshot 127 - Export to File	148

Screenshot 128 - Export to File: Encrypt exported data	148
Screenshot 129 - Creating a new Database Operation	149
Screenshot 130 - Import from SQL Server database	150
Screenshot 131 - Import from SQL Server database: Select the database to import	150
Screenshot 132 - Import from SQL Server database: Decrypt anonymized data	151
Screenshot 133 - Creating a new Database Operation	152
Screenshot 134 - Import from legacy files	152
Screenshot 135 - Creating a new Database Operation	153
Screenshot 136 - Import from legacy file storage	154
Screenshot 137 - Import from legacy file storage: Select file to import	154
Screenshot 138 - Viewing scheduled maintenance jobs	155
Screenshot 139 - Editing a maintenance job	156
Screenshot 140 - Example dialog to edit a scheduled job	156
Screenshot 141 - Maintenance job priorities	157
Screenshot 142 - Firewall rules on Microsoft Windows XP	159
Screenshot 143 - Local security policy window	160
Screenshot 144 - Audit object access Properties	160
Screenshot 145 - Audit process tracking Properties	161
Screenshot 146 - Audit account management properties	162
Screenshot 147 - Audit system events properties	163
Screenshot 148 - Allowed programs in Microsoft Windows Vista or later	164
Screenshot 149 - Local security policy window	165
Screenshot 150 - Audit object access Properties	165
Screenshot 151 - Audit process tracking Properties	166
Screenshot 152 - Audit account management properties	167
Screenshot 153 - Audit system events properties	168
Screenshot 154 - Enable firewall rules in Microsoft Windows Server 2003	169
Screenshot 155 - Firewall rules on Microsoft Windows Server 2008	170
Screenshot 156 - Domain Policy console in Microsoft Windows Server 2003	171
Screenshot 157 - Group Policy Management in Microsoft Windows Server 2008 R2	172
Screenshot 158 - Group Policy Management Editor	173
Screenshot 159 - Predefined rules	174
Screenshot 160 - Predefined rules	175
Screenshot 161 - Configure auto update	181
Screenshot 162 - Update license key	182
Screenshot 163 - Buy now! Button	183

1 Introduction

1.1 About this manual




This user manual is a comprehensive guide aimed at assisting you in configuring and using GFI EventsManager. The user manual contains the following chapters:

CHAPTER	DESCRIPTION
Chapter 1	Introduction An overview of this manual and how GFI EventsManager works.
Chapter 2	Getting Started Describes how to install GFI EventsManager, including system requirements, pre-install actions required and how to upgrade from previous versions.
Chapter 3	Installation Shows how to configure GFI EventsManager for first time use, including how to configure the database backend and how to process event logs for the first time.
Chapter 4	Event browsing Explains how to use the built-in events browser to analyze events stored in the GFI EventsManager database backend, including: <ul style="list-style-type: none">» Default event log queries and custom query builder» Event color-coding» Event finder tool.
Chapter 5	Reporting Describes how to enable the GFI EventsManager ReportPack to create reports that further analyze the events stored in the GFI EventsManager database backend. In addition describes how to configure a user to receive GFI EventsManager Daily Digest email.
Chapter 6	Manage event sources Shows how to add and customize event sources to be monitored.
Chapter 7	Using event processing rules Explains how to use event processing rules.
Chapter 8	Manage rule-sets Describes how to create, edit and delete event processing rules.
Chapter 9	Customizing alerts and actions Shows how to set the alerts and actions that will be triggered on particular events.
Chapter 10	Configuring users and groups Explains how to configure alert recipient parameters including: <ul style="list-style-type: none">» Personal details such as mobile phone number» Normal working hours» Type of alerts that will be sent to every recipient.
Chapter 11	Status monitoring Describes how to analyze the status of GFI EventsManager as well as view statistical information and processed events.

CHAPTER	DESCRIPTION
Chapter 12	Database Operations Explains how to centralize events collected by other remote GFI EventsManager instances and how to optimize database backend performance.
Chapter 13	Miscellaneous Describes miscellaneous options such as permissions, command line operations and licensing.
Chapter 14	Troubleshooting Explains what main sources of information are available to help administrators troubleshoot product issues.
Chapter 15	Glossary Defines technical terms used within GFI EventsManager.

1.2 Conventions used in this manual

The following table contains a description of the common terms and conventions used in this manual:

TERM	DESCRIPTION
	Additional information and references essential for the operation of GFI EventsManager.
	Important notifications and cautions regarding potential issues that are commonly encountered.
	Step by step navigation instructions to access a function.
Bold text	Indicate a control within the user interface, such as nodes, menus and buttons.
<i><Italic text></i>	Replace text within angle brackets. Such as file paths and custom parameters.

For any technical terms and their definitions as used in this manual, refer to [Glossary](#) chapter in this manual.

1.3 About GFI EventsManager

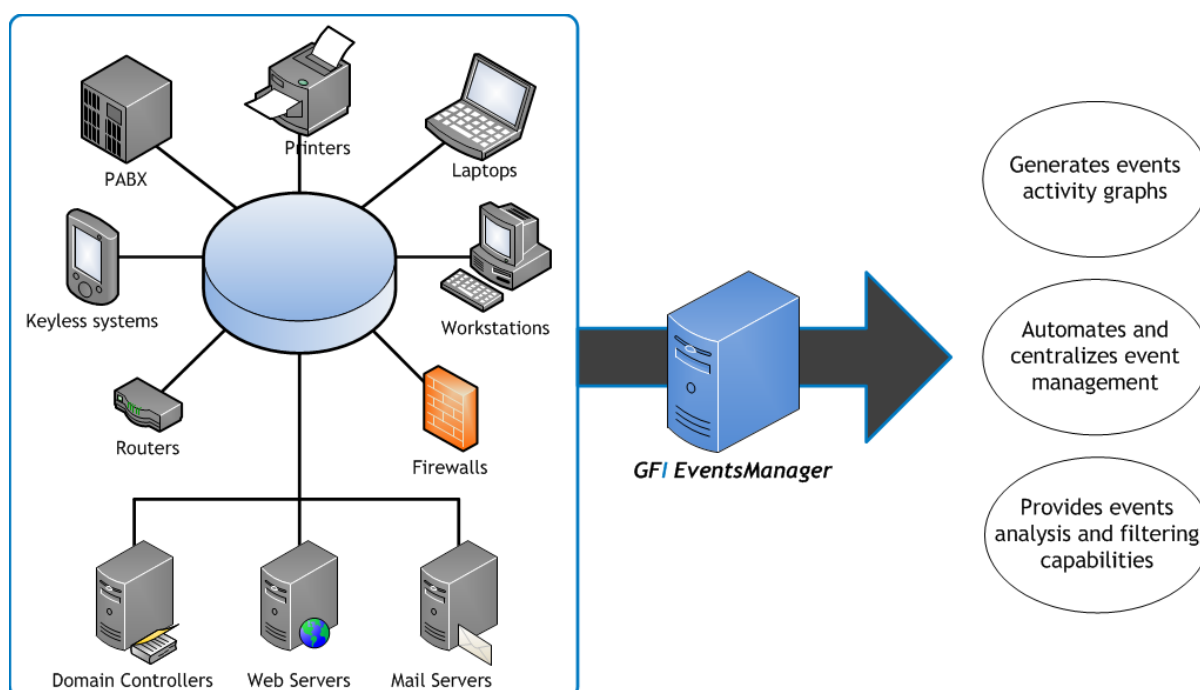


Figure 1 - GFI EventsManager integrates into any existing IT infrastructure

GFI EventsManager is a results oriented event log management solution which integrates into any existing IT infrastructure, automating and simplifying the tasks involved in network-wide events management.

Through the features supported by GFI EventsManager, you are able to:

- » Automatically collect W3C, Syslog, SNMP Traps and Windows event logs from network devices and Windows/Linux/Unix based systems and manage them through one console.
- » Archive collected events in a centralized SQL Server based database backend for future analysis and forensic studies.
- » Automatically transfer events from the database to external files.
- » Filter unwanted events and classify key events through the use of powerful default or custom-built event processing rules.
- » Automate alerting and remedial actions such as the execution of scripts and files on key events.
- » Monitor your network activity and the status of your GFI EventsManager scanning engine through a built-in graphical dashboard.
- » Analyze events through a built-in events browser as well as export these events to CSV files for further processing and report customization.
- » Simplify event forensics through specialized tools which include a built-in event query builder, an event finder tool and an event color-coding tool.
- » Increase event processing power through a high-performance event scanning engine.
- » Generate, schedule as well as email event activity and trend reports through GFI EventsManager ReportPack - the powerful reporting companion tool which ships by default with GFI EventsManager.
- » Monitor the operational health status of your SQL Servers in real-time by processing the activity logs/messages generated by day-to-day SQL Server operations.
- » Monitor Oracle database servers. GFI EventsManager collects and process events generated by Oracle Relational database management systems.
- » Protect data contained in event logs so that confidential information can be encrypted and viewed only by authorized personnel.

1.4 Key Features

Table 1 - Key features

FEATURE	DESCRIPTION
Extended event log support	GFI EventsManager is able to process various event log types including Windows Event Logs, W3C logs, Syslog and SNMP Trap messages. This allows you to collect more data from the different hardware and software systems that are most commonly available on a typical corporate network. For a summary list of hardware and software systems that are supported by GFI EventsManager out-of-the-box refer to: http://kbase.gfi.com/showarticle.asp?id=KBID003302 .
Rule-based event log management	GFI EventsManager ships with a pre-configured set of event processing rules that allow you to filter and classify events collected from a variety of event-log sources. You can run these default rules without performing any configuration or you can choose to customize these rules or create tailored ones that suite your network infrastructure. For a list of event-log sources that can be processed by GFI Events out-of-the-box refer to: http://kbase.gfi.com/showarticle.asp?id=KBID002868 .

FEATURE	DESCRIPTION
Event log scanning profiles	<p>GFI EventsManager enables you to organize event log scanning rules into Scanning Profiles. In a scanning profile, you can configure the set of event log monitoring rules that will be applied to a specific computer or group of computers. The benefits of these profiles include:</p> <ul style="list-style-type: none"> » The simplification product administration tasks by providing a centralized way of tuning event processing rules » Allowing administrators to create different sets of event log rules that suit the roles of scanned event sources and the corporate network environment. For example, you can setup a set of rules which apply only to workstations in a particular department.
Allow granular configuration of rules	Administrators can create an event processing profile that is generic for all computers and a number of separate profiles which complement the generic profile by providing additional and more specialized event log rules on a computer by computer basis.
Translates cryptic Windows events	One major drawback of Windows Event Logs is that they are not user friendly - too cryptic for the user to understand. In fact this is one of the main reasons why only few administrators really peer into Windows Event Logs. GFI EventsManager overcomes this problem by translating event descriptions into a way that is more users friendly and easier to understand.
Enhanced event scanning engine	GFI EventsManager includes an event scanning engine that has been tuned to effectively speed up event scanning for maximum performance. This engine adopts a plug-in based concept that allows the plugging-in of additional features/modules without having to perform physical changes to the existing code - hence more stability without effecting scalability.
Automatic noise reduction	GFI EventsManager identifies and removes unwanted event data (such as noise and background process generated events) providing you with only the relevant, usable data. Hence facilitates event forensics by reducing the amount of events to be analyzed.
Enhanced real-time actions	GFI EventsManager can generate alerts or trigger actions such as script execution when key events are detected. You can alert one or more people in various ways including: email, network messages, and SMS notifications sent through an email-to-SMS gateway or service. Actions can be configured to trigger on event classification or by configuring specific conditions in event processing rules.
Advanced event filtering features	<p>GFI EventsManager ships with a number of event filtering features including:</p> <ul style="list-style-type: none"> » Pre-configured event queries and a custom event query builder: The pre-configured event queries allow you to sift event log data and browse only the required events - without deleting any records from your database backend. The built-in event query builder allows you to create your own custom event queries. » Event color-coding capabilities: Through this feature you can selectively color particular events in specific colors. This way during log browsing you can easily identify important events through their color. » Event finder tool: With this tool you can quickly locate important events by providing specific search criteria such as event type.
Event centralization	GFI EventsManager enables you to monitor and manage events generated by Windows/Linux/Unix systems, network devices and software applications through a single user console.
User access privileges	GFI EventsManager enables you to assign management console access privileges on a user-by-user basis. This means that you can allow specific users to access the GFI EventsManager console for event-browsing only and at the same time allow other more privileged users to access and change the GFI EventsManager configuration settings.

FEATURE	DESCRIPTION
SQL Server audit	GFI EventsManager enables you to automatically monitor the operational health status of your SQL Servers. This is achieved by processing in real-time the activity logs/messages generated by day-to-day SQL Server operations. SQL server activity that is monitored includes server startup, login activity, backups, server-side traces and more. Additionally, GFI EventsManager can also alert you via email, network or SMS notifications on key events like server shutdown and consecutive failed logins.
Oracle Server audit	GFI EventsManager enables you to automatically monitor the activity and the operational health status of your Oracle Servers. Within GFI EventsManager you can configure Oracle servers to log audit events. Oracle audit events are stored in a specific table on the Oracle server. GFI EventsManager collects and process these events. GFI EventsManager can also alert you via email, network or SMS notifications when specific events occur.
Database operations (WAN Connector)	The Database Operations module enables you to collect events data from GFI EventsManager installations on multiple sites and locations across your network into a central database. This add-on integrates and centralizes events collected and processed and allows you to backup/restore events on demand. Through Database Operations you can manage the size of the database - without the need for manual intervention - not only through centralization but by also being able to export events and back them up as needed.
Management Information Base	Management Information Base (MIBs) contains definitions and device information that are provided by device manufacturers. GFI EventsManager ships with MIB definitions for the following vendors: Cisco, 3Com, IBM, HP, Check Point, Alcatel, Dell, Netgear, SonicWall, Juniper Networks, Arbor Networks, Oracle, Symantec, Allied Telesis and others. GFI EventsManager also allows you to edit the MIB tree.
Anonymization	GFI EventsManager has built-in security features that help you encrypt your data for legal compliance purposes. Anonymizing your data helps you hide personal information from the Dashboard, Events Browser and exported events. To view these events, a decryption password is required.

1.5 How does GFI EventsManager work?

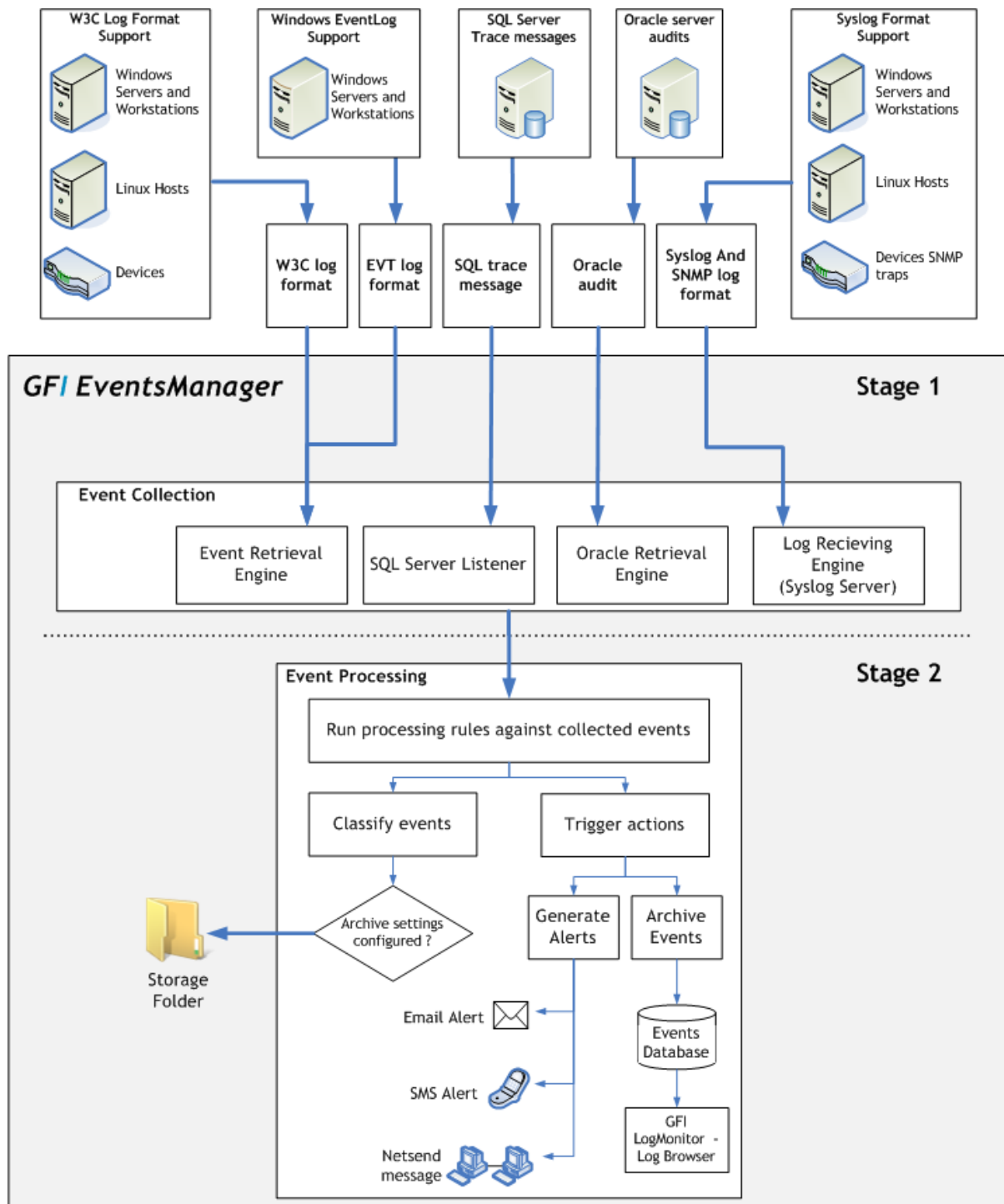


Figure 2 - The GFI EventsManager operational stages

The operational functionality of GFI EventsManager is divided into two stages described below:

1.5.1 Stage 1: Event Collection

During the Event Collection stage, GFI EventsManager collects logs from specific event sources. This is achieved through the use of two event collection engines: The **Event Retrieval Engine** and the **Event Receiving Engine**.

Table 2 - GFI EventsManager engines

ENGINE	DESCRIPTION
The Event Retrieval Engine	<p>The Event Retrieval Engine is used to collect Windows Event Logs and W3C logs from networked event sources. During the Event Collection process this engine will:</p> <ol style="list-style-type: none"> 1. Log-on to the event source(s) 2. Collect events from the source(s) 3. Send collected events to the GFI EventsManager Server 4. Log-off from the event source(s). <p>The Event Retrieval Engine collects events at specific time intervals. The event collection interval is configurable from the GFI EventsManager management console</p>
The SQL Server Listener	<p>The listener receives trace messages from the scanned Microsoft SQL Server in real time. On receipt, EventsManager processes the message immediately.</p>
The Oracle Retrieval Engine	<p>The Oracle Retrieval Engine connects periodically to Oracle servers and collects audits from a specific auditing table. Similar to the Microsoft Windows Event Retrieval Engine, GFI EventsManager processes events generated by the Oracle server.</p>
Log Receiving Engine	<p>The Event Receiving Engine acts as a Syslog and an SNMP Traps server; it listens and collects Syslog and SNMP Trap events/messages sent by various sources on the network. As opposed to the Event Retrieval Engine, the Event Receiving Engine receives messages directly from the event source; therefore it does not require to remotely log-on to the event sources for event collection. Further to this, Syslog and SNMP Trap events/messages are collected in real-time and therefore no collection time intervals need to be configured.</p> <p>By default, the Event Receiving Engine listens to Syslog messages on port 514 and to SNMP Trap messages on port 162. Both port settings are however customizable via the GFI EventsManager management console.</p>

1.5.2 Stage 2: Event Processing

During this stage, GFI EventsManager will run a set of Event Processing Rules against collected events. Event Processing rules are instructions that:

- » Analyze the collected logs and classify processed events as Critical, High, Medium, Low or Noise (unwanted or repeated events)
- » Filter events that match specific conditions
- » Trigger email, SMS and network alerts on key events
- » Trigger remediation actions such as the execution of executable files or scripts on key events
- » Optionally archive collected events in the database backend.

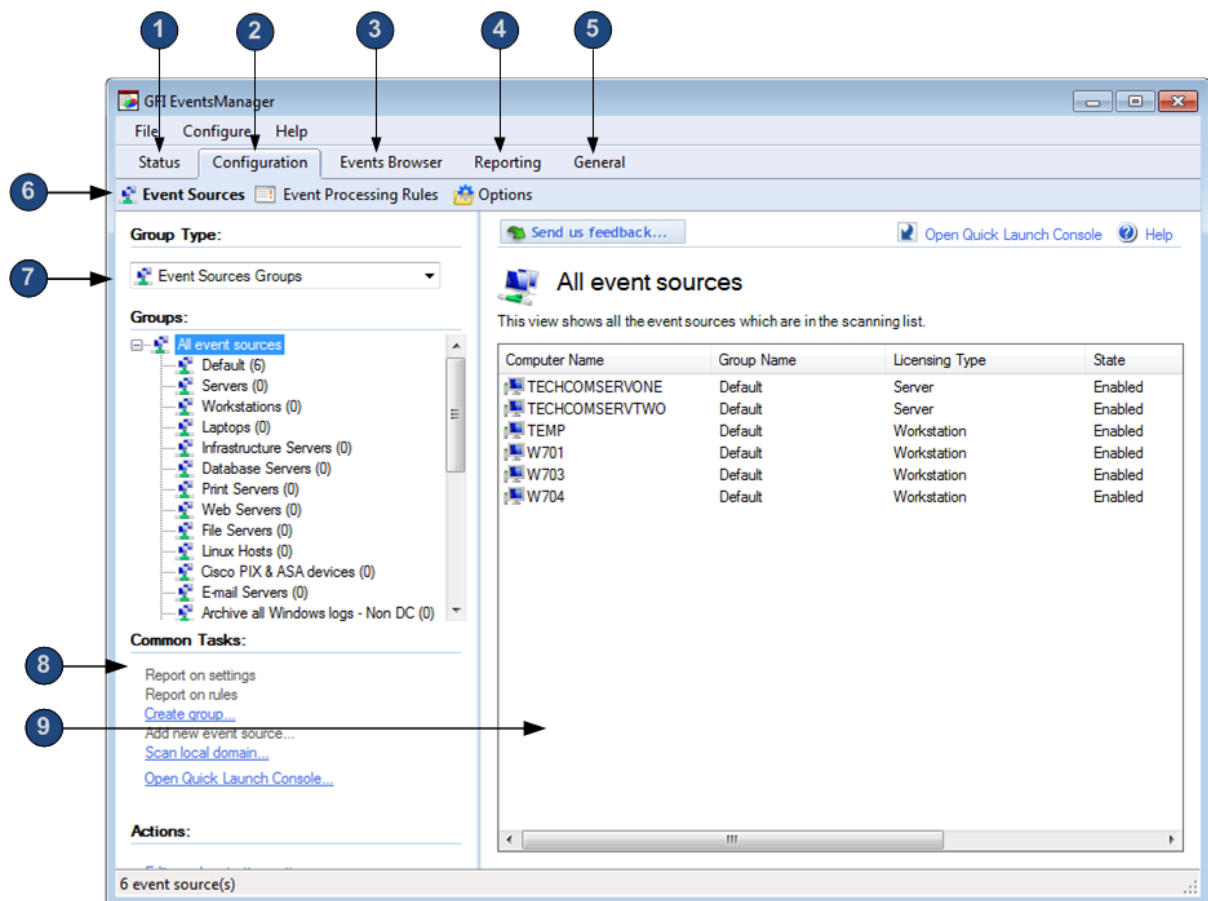
GFI EventsManager can be configured to archive events without running Event Processing rules. In such cases, even though no rules will be applied against collected logs, archiving will still be handled by the Event Processing stage.

After processing the rules, GFI EventsManager can be configured to store the collected events in a storage folder. The administrator can configure the path of the storage folder and configure which events are stored. This function will minimize database growth, and allows the administrator to store only important events in the database.



Some of the key modules in GFI EventsManager must run under administrative privileges. For more information on these modules refer to:
<http://kbase.gfi.com/showarticle.asp?id=KBID001122>.

1.6 Navigating the GFI EventsManager management console



Screenshot 1 - The GFI EventsManager management console

SECTION	DESCRIPTION
1	Status option Use this option to view the status of GFI EventsManager and statistical information on processed logs.
2	Configuration option Use this option to access and configure the main event processing options.
3	Events Browser Use this option to browse the events stored in the GFI EventsManager database backend.
4	Reporting Use this option to access GFI EventsManager reporting features, create new reports and schedule reports to be generated.
5	General options Use this option to check for product updates, as well as view version and licensing details.
6	Tab options Use the Tab options to access and configure GFI EventsManager operational parameters.
7	Group Type Use this drop-down to switch between event log source groups (i.e. Computer and Database Servers Groups).
8	Left pane Use this pane to navigate through the additional configuration options provided in GFI EventsManager.
9	Right pane Event browsing and parameter configuration pane.

2 Getting Started

2.1 Introduction

This chapter provides information about the type of different log formats supported by GFI EventsManager. For more information, refer to the sections below within this chapter:

- » What is a computer log?
- » What are Windows Event Logs?
- » What are W3C logs?
- » What are Syslogs?
- » What are SNMP Traps?
- » What are SQL Server audit logs?
- » What are Oracle Server audit logs?

2.2 What is a computer log?

A computer log is a collection of event entries. These entries provide an audit trail of information related to the activity of a network or computer system. In fact, computer logs are recorded in a certain scope to provide information suitable for forensic analysis. The computer log may be a binary file as in the case of Windows logs, or text-based files as in the case of Syslog or W3C logs.

Such events include various details such as the date and time the event occurred and a related description. Event entries are often stored in chronological order to facilitate event browsing and forensic analysis.

2.3 What are Windows Event Logs?




Windows Event Logs are a systematic recording of computer related events that occurred within computer systems and networks running on Windows Operating Systems. In systems running on Windows 2000/XP/2003/VISTA, events are recorded and organized in 3 default event logs:



- » Application log
- » Security log
- » System log.

Computers with specialized network roles such as domain controllers and DNS servers allow the logging of events to additional (default) logs such as:

- » Directory service log
- » File Replication service log
- » DNS server log.

Windows Event Logs contain the following types of events:

EVENT TYPE	DESCRIPTION
 Error	Error events indicate that a significant problem, such as loss of data or functionality has occurred. For example an Error event is recorded every time that a service or driver fails to load during startup.
 Warning	Warnings indicate events that are not necessarily significant, but which may possibly cause future problems. For example, a Warning event is recorded every time that disk space runs low.
 Information	Information events describe the successful operation of an application, driver, or service. For example, an Information event is recorded every time that a network driver loads successfully.

EVENT TYPE	DESCRIPTION
 Success Audit	Success audit events indicate security access attempts that were successful. For example, a Success Audit event is recorded every time that a user successfully logs on to his Windows based workstation.
 Failure Audit	Failure audit events indicate security access attempts that failed. For example, a Failure audit event is recorded every time that a user fails to access a network drive.

2.4 What are W3C logs?

W3C logs are used mainly by web servers to log web related events including web logs. W3C logs are recorded in text-based flat files using any one of the two W3C logging formats currently available:

- » W3C Common Log file format
- » W3C Extended Log File format.

The W3C common log file format was the first format to be released and to date it is still the default format used by a variety of popular web servers including Apache. There is however one downside - the information about each server transaction is fixed and does not provide for certain important fields such as referrer, agent, transfer time, domain name, or cookie information. To overcome this problem, the W3C Extended log file format was released. This newer type of log is in customizable ASCII text-based format, permitting a wider range of data to be captured. The W3C Extended log file format is the default log file format used by Microsoft Internet Information Server (IIS).

A sample of the information typically recorded in a W3C extended type log is shown below:

```
#Version: 1.0
#Date: 04-Sep-2009 00:00:00
#Fields: time cs-method cs-uri
00:34:23 GET /WebSRV/Pg_Snippet.html
12:21:16 GET /WebSRV/ Button_pg.html
12:45:52 GET /WebSRV/ Login_Pg.html
12:57:34 GET /WebSRV/ Error_msg.html
```

2.5 What are Syslogs?

Syslog is the standard for logging messages, such as system events, in an IP network. The Syslog standard is most commonly used for the logging of events by computer systems running on UNIX and Linux as well by network devices and appliances such as Cisco routers and the Cisco PIX firewall. Syslog events are not directly recorded by applications running on the computer systems. Whenever an event is generated, the respective computer will send a small textual message (known as Syslog message) to a dedicated server commonly known as 'Syslog server'. The Syslog server will then save the received message into a log file. Syslog messages are generally sent as clear text; however, an SSL wrapper can be used to provide for a layer of encryption.

Syslog is typically used for computer system management and security auditing. While it has a number of shortcomings, its big plus is that Syslog is supported by a wide variety of devices and receivers. Because of this, Syslog can be used to integrate log data from many different types of systems into a central repository using the Syslog server as a log aggregator.

The Syslog daemon handles the recording of Syslog messages/events in log files. The Syslog message is composed of two main parts:

1. The ‘header’ which contains date/time information as well as the IP or computer name from where the message has originated.
2. The “message” which includes the program or subsystem name and the message itself, separated by a colon. The following is an example of a Syslog message:

```
Sep 4 10:10:10 10.245.2.11 foo[421]: this is a message from
WebSRV
```

2.6 What are SNMP Traps?

SNMP Traps are used by network management systems to monitor network devices (such as routers, firewalls or switches) for conditions that require administrative attention. This includes monitoring device uptime, inventories of operating system versions and collecting interface information. SNMP enabled devices do not record event messages locally but instead these transmit event details to an SNMP Trap server which analyzes these occurrences and alert systems administrators on key events.

GFI EventsManager includes its own SNMP Trap server that captures SNMP messages and informs systems administrators of network device failures and other critical events. GFI EventsManager supports various versions of SNMP Traps including SNMP versions 1, 2 and 3 (the encoded version).

2.7 What are SQL Server audit logs?

Microsoft SQL Server generates event logs that allow the network administrator to monitor database activity. GFI EventsManager allows you to process the activity logs generated by day-to-day SQL Server operations such as server startup or on key events such as failed logons. Alerts can also be created when key events such as consecutive login failure is identified in Microsoft SQL Server audit logs.

2.8 What are Oracle Server audit logs?

Oracle Servers can be configured to generate event logs that enable administrators to monitor activity. GFI EventsManager can be configured to collect and process these events. Oracle Server auditing includes data related to:

- » Data manipulation actions
- » User access actions
- » User privileges
- » Database schema
- » Database structure.

3 Installation

3.1 Introduction

This chapter provides information about the different deployment scenarios supported by GFI EventsManager and information required to install and run the product for the first time. It contains the following sections:

- » Where can I install GFI EventsManager on my network?
- » System requirements
- » Upgrading from a previous version
- » Installation procedure
- » Running GFI EventsManager for the first time

3.2 Where can I install GFI EventsManager on my network?

GFI EventsManager can be installed on any computer which meets the minimum system requirements irrespective of the location on your network.



If you want to collect event logs from Microsoft Windows Vista or later, GFI EventsManager must be installed on a machine running Microsoft Windows Vista, 7 or Server 2008.

Use GFI EventsManager to manage the events generated:

- » By the same computer where it is installed
- » By all the computers that are reachable from the computer on which it is installed.

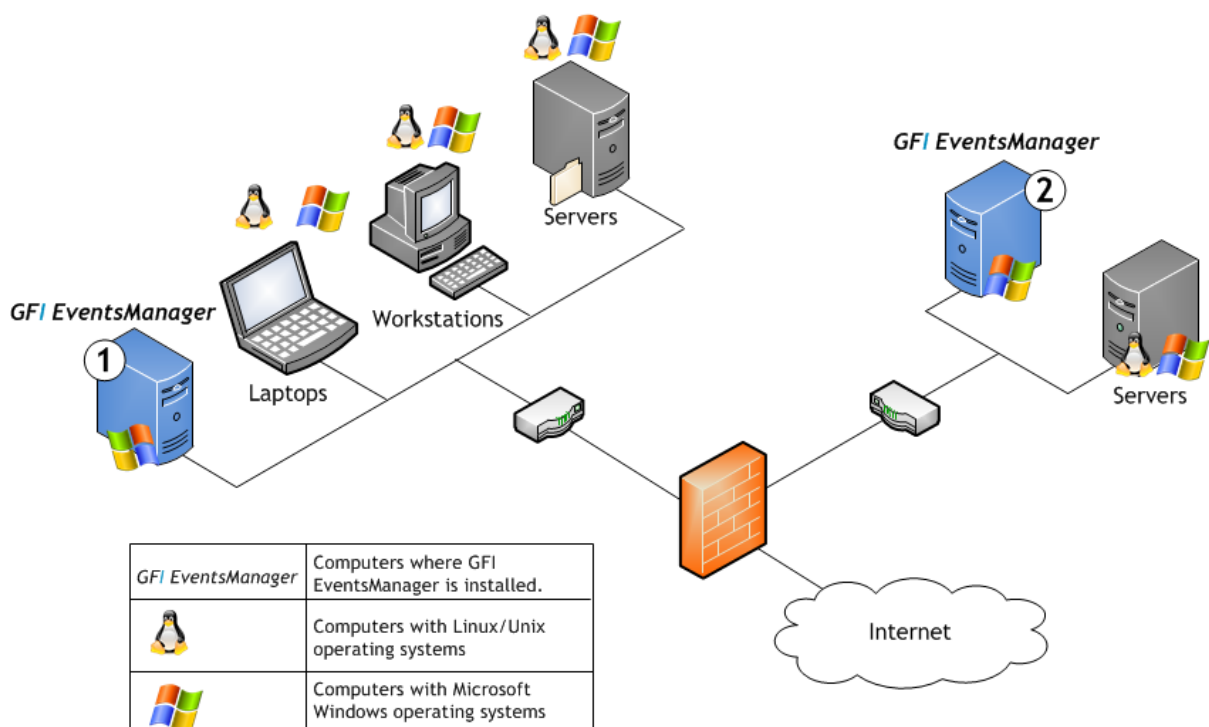


Figure 3 - GFI EventsManager deployment scenario

GFI EventsManager can be deployed in a:

- » LAN - Monitor the activity of internal servers and workstations/end points
- » DMZ - Monitor and manage the events generated on your servers.

3.2.1 Deploying GFI EventsManager - Local Area Network

GFI EventsManager can be deployed on Windows based networks as well as on mixed environments where Linux and UNIX systems are being used as well.

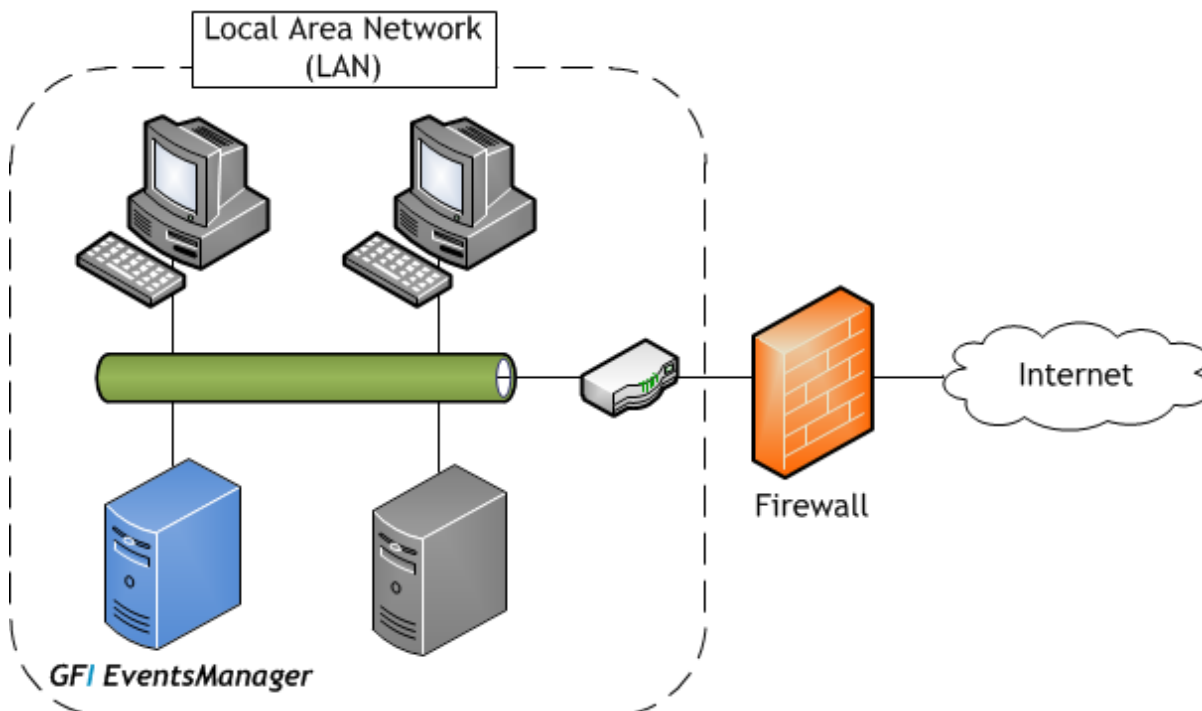


Figure 4 - Deployment of GFI EventsManager in LAN

When installed on a Local Area Network (LAN) GFI EventsManager can manage Windows events, W3C event logs, Syslog messages, SNMP Trap and SQL Server audit messages generated by any hardware or software that is connected to the LAN, including:

Table 3 - Devices supported by GFI EventsManager

DEVICE	EXAMPLE
Workstations and laptops	End-user computers and systems.
Servers	Web servers, Mail servers, DNS servers and more.
Network devices	Routers, switches and any other device that generates performance logs.
Software	Including GFI EndPointSecurity, GFI LanGuard and other applications that generate logs.
Specialized Services	Microsoft Internet Information Server - IIS.
PABXs, Keyless Access Systems, Intrusion detections systems and more	GFI EventsManager enables you to monitor any device that is attached to the network.

When installed on a LAN, GFI EventsManager can also be used to collect events from hardware and software systems deployed on a Demilitarized Zone (DMZ). Since a firewall or a router usually protects this zone with network traffic filtering capabilities, you must make sure that:

1. The communication ports used by GFI EventsManager are not blocked by the firewall. For more information on the communication ports used by GFI EventsManager refer: <http://kbase.gfi.com/showarticle.asp?id=KBID002770>.
2. That GFI EventsManager has administrative privileges over the computers that are running on the DMZ.

3.2.2 Deployment of GFI EventsManager on a demilitarized zone

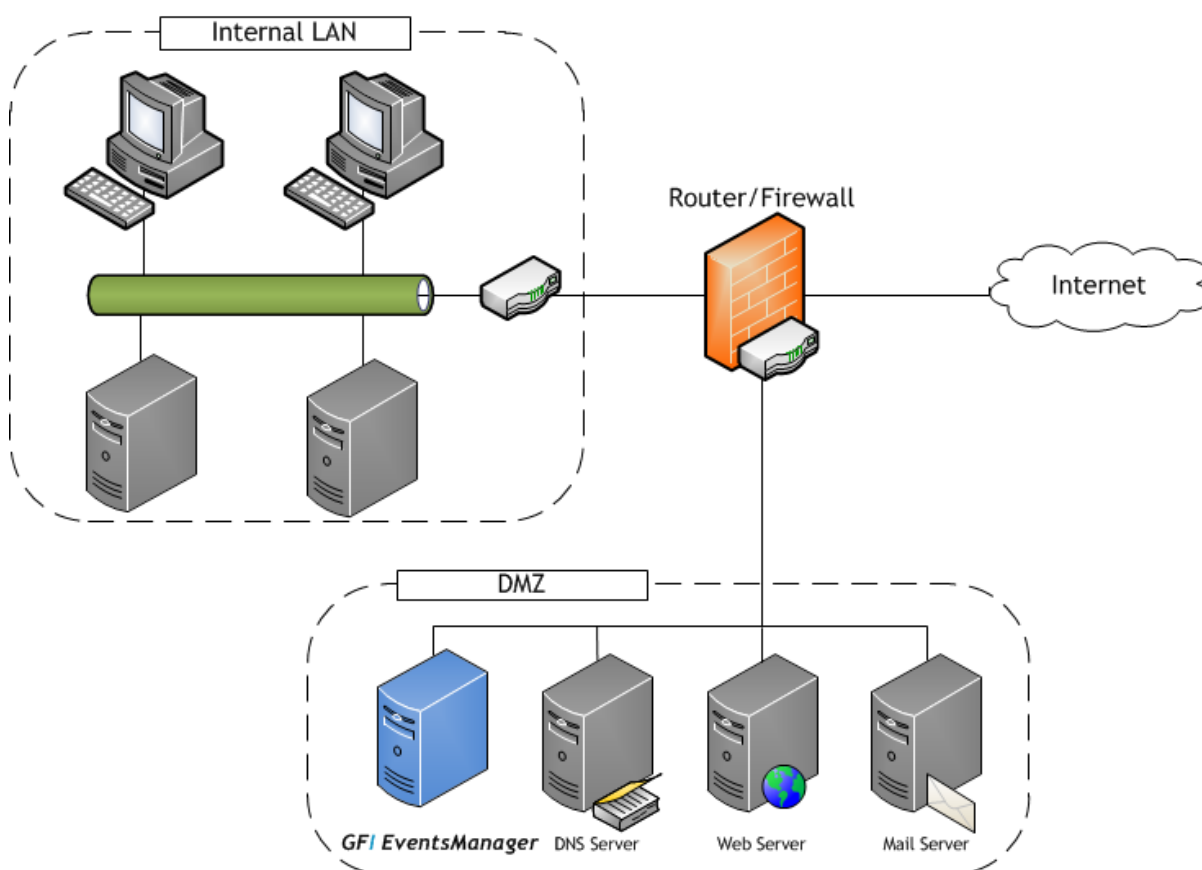


Figure 5 - The DMZ sits between the internal LAN and the Internet

GFI EventsManager can also be deployed on a Demilitarized Zone (DMZ). This is the neutral network which sits between the “internal” corporate network and the “outside world” (Internet). The deployment of GFI EventsManager on a DMZ helps you automate the management of events generated by DMZ hardware and software systems; such as:

Table 4 - Benefits of installing GFI EventsManager in DMZ

DMZ AUTOMATION	DESCRIPTION
Automate management of Web and Mail server events	<p>DMZ networks are normally used for the running of hardware and software systems that have internet specific roles such as HTTP servers, FTP servers, and Mail servers.</p> <p>Hence, you can deploy GFI EventsManager to automatically manage the events generated by:</p> <ul style="list-style-type: none"> » Linux/Unix based web-servers including the W3C web-logs generated by Apache web-servers on LAMP web platforms. » Windows based web-servers including the W3C web-logs generated by Microsoft Internet Information Servers (IIS). » Linux/Unix and Windows based mail-servers including the Syslog auditing services messages generated by Sun Solaris v. 9 or later.
Automate management of DNS server events	<p>If you have a public DNS server, there's a good chance that you are running a DNS server on the DMZ. Hence you can use GFI EventsManager to automatically collect and process DNS server events including those stored in your Windows' DNS Server logs.</p>

DMZ AUTOMATION	DESCRIPTION
Automate management of network appliance events	<p>Routers and firewalls are two network appliances commonly found in a DMZ. Specialized routers and firewalls (e.g. Cisco IOS series routers) not only help protect your internal network, but provide specialized features such as Port Address Translation (PAT) that can augment the operational performance of your systems.</p> <p>By deploying GFI EventsManager on your DMZ, you can collect the events generated by such network appliances. For example, you can configure GFI EventsManager to act as a Syslog Server and collect in real-time the Syslog messages generated by Cisco IOS routers.</p>

3.3 System requirements

3.3.1 Hardware requirements

Table 5 - Hardware requirements

HARDWARE COMPONENT	SPECIFICATION
Processor	2.5 GHz dual core or higher.
RAM	3 GB.
Hard disk	10 GB free space.



Hard disk size depends on your environment, the size specified in the requirements is the minimum required to install and archive events.

3.3.2 Software requirements

Table 6 - Software requirements: Operating system

OPERATING SYSTEM (x86 OR x64)
Windows Server 2008 - Standard or Enterprise.
Windows Server 2008 R2 - Standard or Enterprise.
Windows Server 2003 SP2 - Standard or Enterprise.
Windows 7 - Enterprise, Professional or Ultimate.
Windows Vista SP1 - Enterprise, Business or Ultimate.
Windows XP Professional SP3.
Windows SBS 2008.
Windows SBS 2003.

Table 7 - Software requirements: Other components

OTHER COMPONENTS
Microsoft .NET framework 4.0.
Microsoft Data Access Components (MDAC) 2.8 or later.
A mail server (when email alerting is required).



Microsoft Data Access Components (MDAC) 2.8 can be downloaded from <http://www.microsoft.com/Downloads/details.aspx?familyid=6C050FE3-C795-4B7D-B037-185D0506396C&displaylang=en>

3.3.3 Event source settings

The below table describes the configuration required for event sources:

Table 8 - System requirements: Event source settings

LOG TYPE	DESCRIPTION
Windows event log processing	Enable remote registry.
W3C log processing	The source folders must be accessible via Windows shares.

LOG TYPE	DESCRIPTION
Syslog and SNMP Traps processing	Configure sources/senders to send messages to the computer/IP where GFI EventsManager is installed.
Scanning machines with Windows Vista or later	Install GFI EventsManager on a computer running Windows Vista or later.
System auditing	Enable auditing on event sources. For information, refer to Miscellaneous .

3.3.4 Ports and permissions

The table below specifies the Ports required by GFI EventsManager:

Table 9 - System requirements: Ports and protocols

PORT	PROTOCOL	DESCRIPTION
135	UDP and TCP	Target machines use this port to publish information regarding available dynamic ports. GFI EventsManager uses this information to be able to communicate with the target machines.
139 and 445	UDP and TCP	Used by GFI EventsManager to retrieve the event log descriptions from target machines.
162	UDP and TCP	Used by GFI EventsManager to receive SNMP traps. Ensure that this port is open on the machine where GFI EventsManager is installed
514	UDP and TCP	Used by GFI EventsManager to receive SYSLOG messages.
1433	UDP and TCP	Used by GFI EventsManager to communicate with the SQL Server database backend. Ensure that this port is enabled on Microsoft SQL Server and on the machine where GFI EventsManager is installed.
1521	UDP and TCP	Used to collect Oracle Server audit logs. Port 1521 is the default port for this connection. If the port is changed manually in the Oracle Listener's configuration, adjust firewall settings accordingly.
49153	UDP and TCP	Used by GFI EventsManager to collect events from event sources with Microsoft Windows Vista or Microsoft Windows 7.

The table below specifies the Firewall Permissions required by GFI EventsManager:

Table 10 - System requirements: Firewall permissions

FIREWALL PERMISSIONS AND AUDIT POLICIES	MICROSOFT WINDOWS SERVER 2008	MICROSOFT WINDOWS SERVER 2003	MICROSOFT WINDOWS XP	MICROSOFT WINDOWS VISTA	MICROSOFT WINDOWS 7
Remote Event Log Management	Enable	Not applicable	Not applicable	Enable	Enable
File and Printer sharing	Enable	Enable	Enable	Enable	Enable
Network discovery	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Object access	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Process tracking	Enable	Not applicable	Not applicable	Enable	Enable
Audit policy: Audit account management	Enable	Enable	Enable	Enable	Enable
Audit policy: Audit system events	Enable	Enable	Enable	Enable	Enable



For more information, refer to [Enabling permissions on events sources manually](#) or [Enabling permissions on event sources automatically](#).

3.3.5 Monitoring event logs from Microsoft Windows Vista or later

GFI EventsManager cannot be installed on Microsoft Windows XP to monitor events of Microsoft Windows Vista or later. Microsoft Windows Vista and Microsoft Windows 7 introduced extensive structural changes in event logging and event log management. The most important of these changes include:

- » A new XML-based format for event logs. This provides a more structured approach to reporting on all system occurrences.
- » Event categorization in four distinct groups: Administrative, Operational, Analytic and Debug
- » A new file format (evtx) that replaces the old evt file format.

Due to these changes, to collect and process event logs from Microsoft Windows Vista or later, GFI EventsManager must be installed on a system running:

- » Microsoft Windows Vista
- » Microsoft Windows 7
- » Microsoft Windows Server 2008.



Windows XP events can be collected when GFI EventsManager is installed on Microsoft Windows Vista or later machines.



When GFI EventsManager is using a non-domain account to collect events from Microsoft Vista machines or later, target machines must have **User Account Control (UAC)** disabled. For more information on how to disable UAC, refer to [Disable UAC to scan target machines](#) section in this manual.

3.4 Upgrading from a previous version

Upgrading from older versions is not possible due to the underlying operational and processing technology subsystems.

You will still however be able to run an older version of GFI EventsManager on the same machine on which a newer version of GFI EventsManager is installed since there are no conflicts between the older and the newer versions.

You can also export events from an older version of GFI EventsManager and import the data in the new one, using Database Operations. For more information, refer to [Database Operations](#).

3.5 Firewalls and Anti-virus software

If firewall(s) are enabled and anti-virus software installed on the computer where GFI EventsManager is running, make sure that:

- » Traffic is not blocked on the ports in use by GFI EventsManager
- » **esmui.exe** and **esmpoc.exe** are allowed access through the firewall(s)
- » GFI EventsManager folders are excluded from real-time anti-virus scanning.

For more information on the ports and permissions that must be enabled, refer to [Ports and permissions](#).

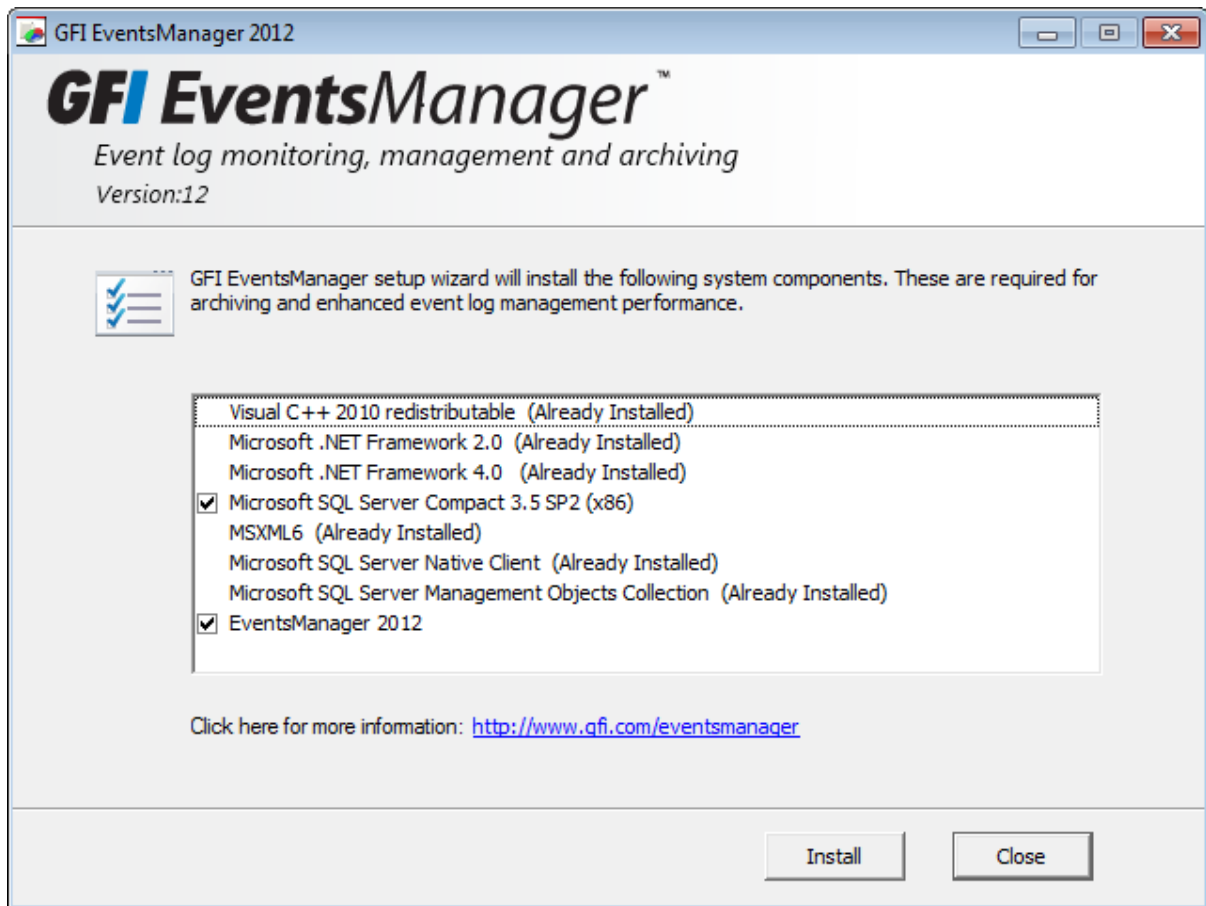
3.6 Computer identification considerations

GFI EventsManager identifies computers via computer name or IP. If NETBIOS-compatible computer names are used, ensure that your DNS service is properly configured for name resolution. Unreliable name resolution downgrades overall system performance. If you disable NETBIOS over TCP/IP, you can still use GFI EventsManager, however you must specify computer name by IP.

3.7 Installation procedure

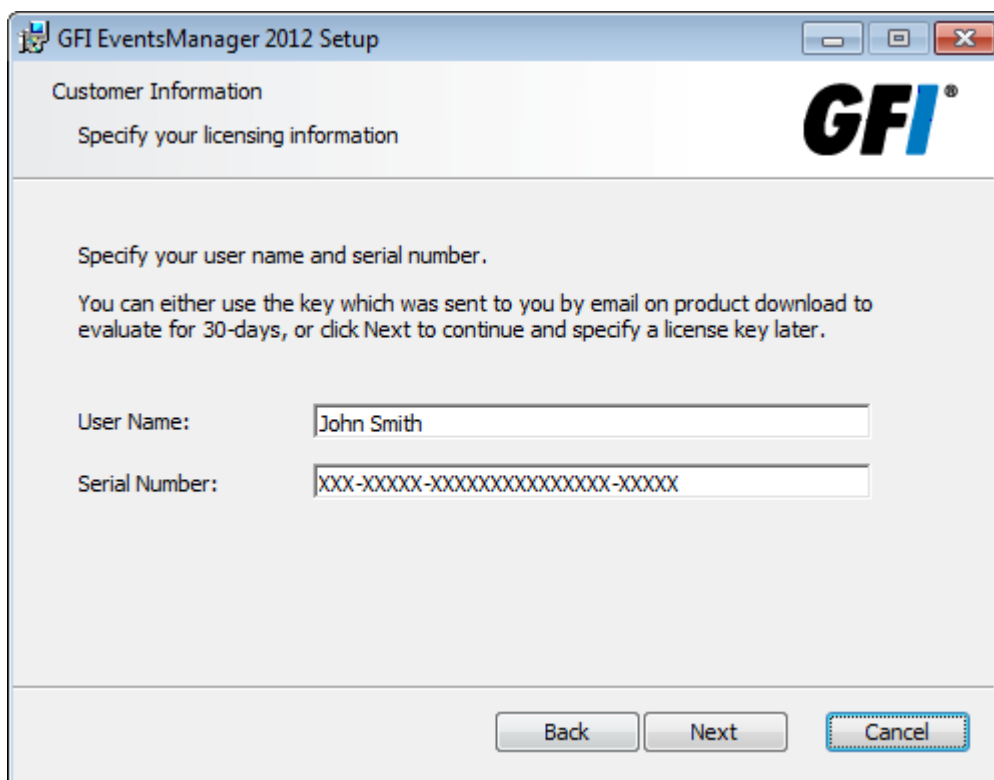
To install GFI EventsManager:

1. Close all running applications and log on the target computer using an account which has local administrative privileges.
2. Double-click GFI EventsManager setup file.



Screenshot 2 - Pre-requisite check

3. GFI EventsManager will check your system for components that are not already installed. Click **Install** to begin the installation.
4. Click **Next** at the wizard welcome step.
5. Read the licensing agreement carefully. Select 'I accept the terms in the License Agreement'. Click **Next**.



Screenshot 3 - Customer and License detail screen

6. Key in your name and serial number. Click **Next**.



Screenshot 4 - Logon information screen

7. Key in a user name and password of a domain administrator account. Click **Next**.

8. Specify an alternative installation path or click **Next** to leave as default.

9. Click **Install**.

3.8 Running GFI EventsManager for the first time

After installing GFI EventsManager, the Management Console is launched automatically. To launch GFI EventsManager manually, click **Start ► All Programs ► GFI EventsManager ► Management Console**.

Follow the steps outlined below to configure GFI EventsManager for first time use:

- » **Step 1: Launch events processing**
- » **Step 2: Analyze events and generate reports.**

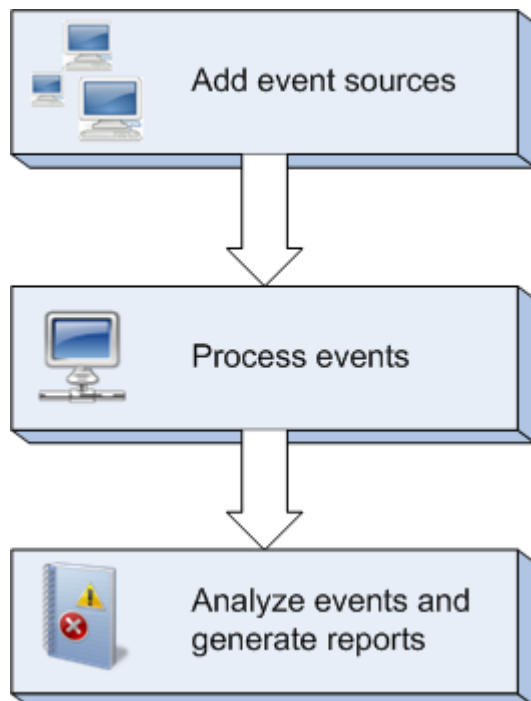
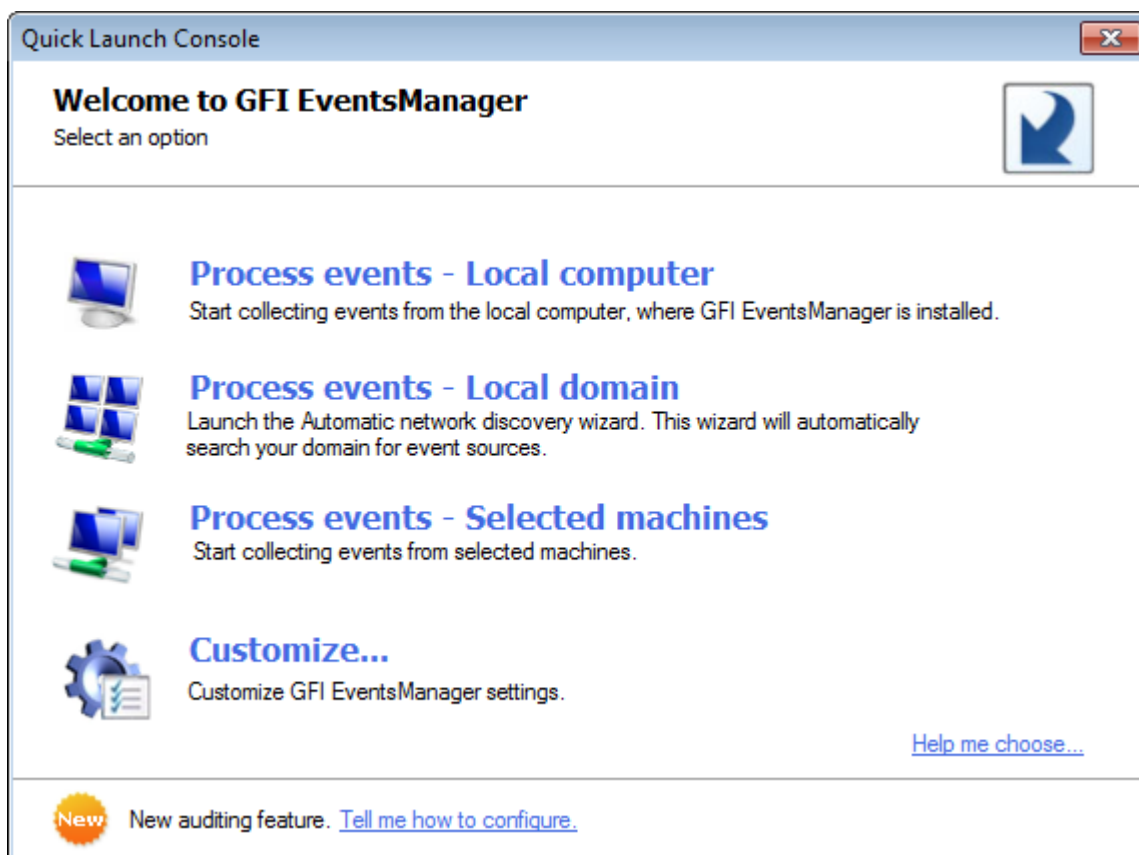


Figure 6: Running GFI EventsManager for the first time

3.8.1 Step 1: Launch events processing

This section contains information about:

- » Processing events from the local computer
- » Processing events from the local domain
- » Processing events from selected machines



Screenshot 5 - Quick Start Dialog

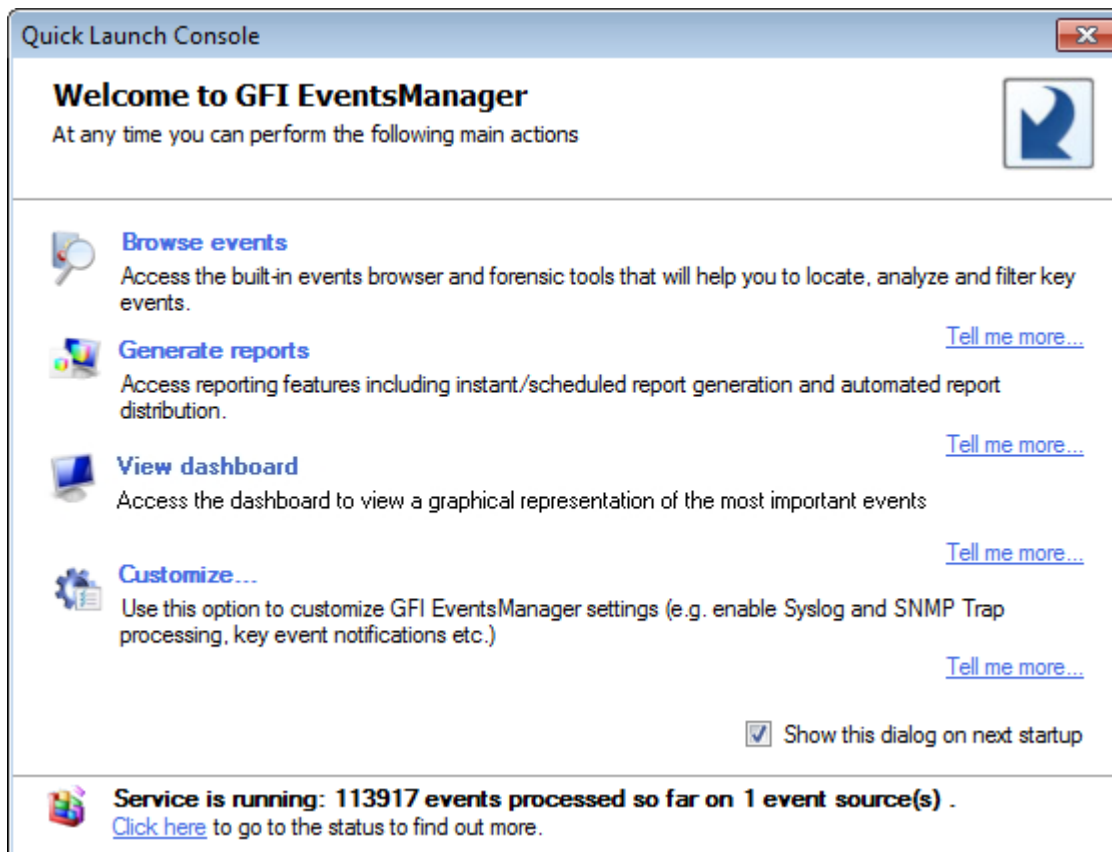
From the **Quick Launch Console**, select one of the following options:

OPTION	DESCRIPTION
Process events - local computer	Start collecting events from the local computer, where GFI EventsManager is installed. For more information refer to Processing events from the local computer .
Process events - local domain	Launch the Automatic network discovery wizard. This wizard will automatically search your network for event sources. For more information refer to Processing events from the local domain .
Process events - selected machines	Add event sources manually without using the wizard. For more information refer to Processing events from selected machines .
Customize	Customize settings of: <ul style="list-style-type: none"> » Events sources and log types » Event processing rules » Database operations » Users and groups » Alerting options.

Processing events from the local computer

To process event logs from the local machine:

1. From **Quick Launch Console**, click **Process events - local computer**. GFI EventsManager will start to collect events from the local machine immediately.



Screenshot 6 - Events processed from local machine

On completion, the number of events that have been processed is displayed in the information bar as illustrated in the screenshot above.

Processing events from the local domain

The **Network discovery wizard** searches the entire network for computers and servers. This will assist in adding network computers as GFI EventsManager event sources. To launch the Network discovery wizard:

1. From the **Quick Launch Console** , click **Process events - Local domain**.

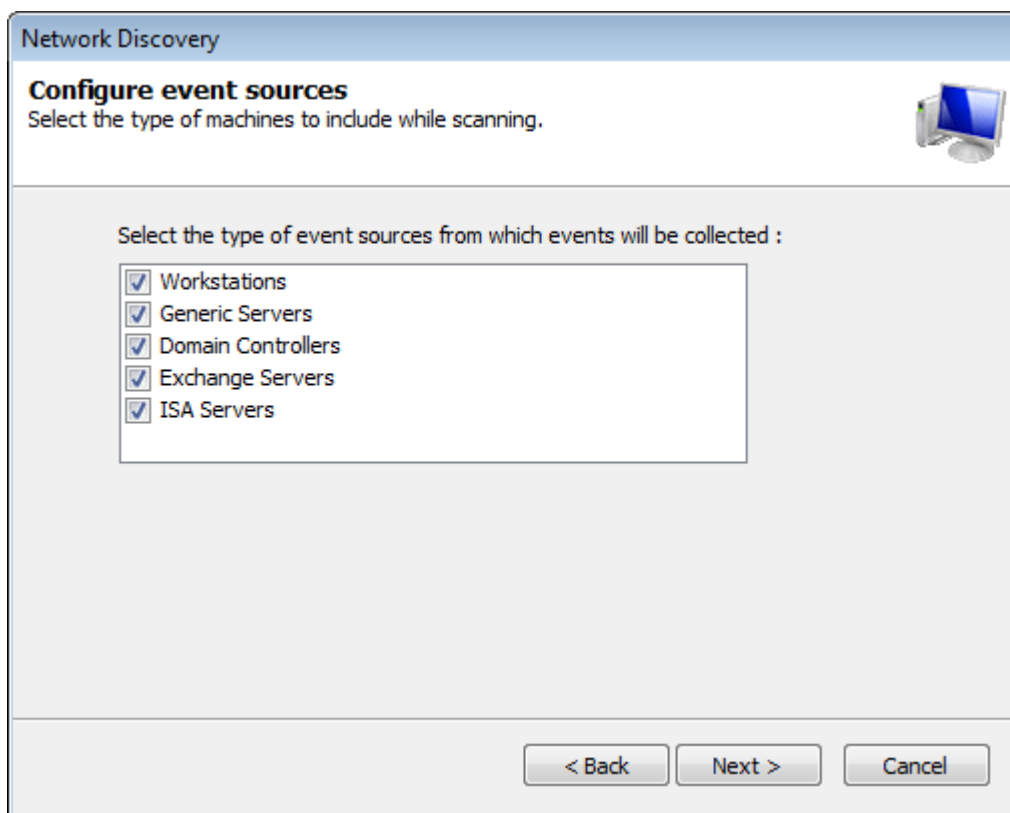


The wizard can also be launched from **Configuration ► Event Sources**, right click **All event sources** and select **Scan local domain**.



If synchronization options are configured, **Process events - Local Domain** is disabled. For more information refer to [Edit synchronization options](#).

2. In the Welcome screen, click **Next**.



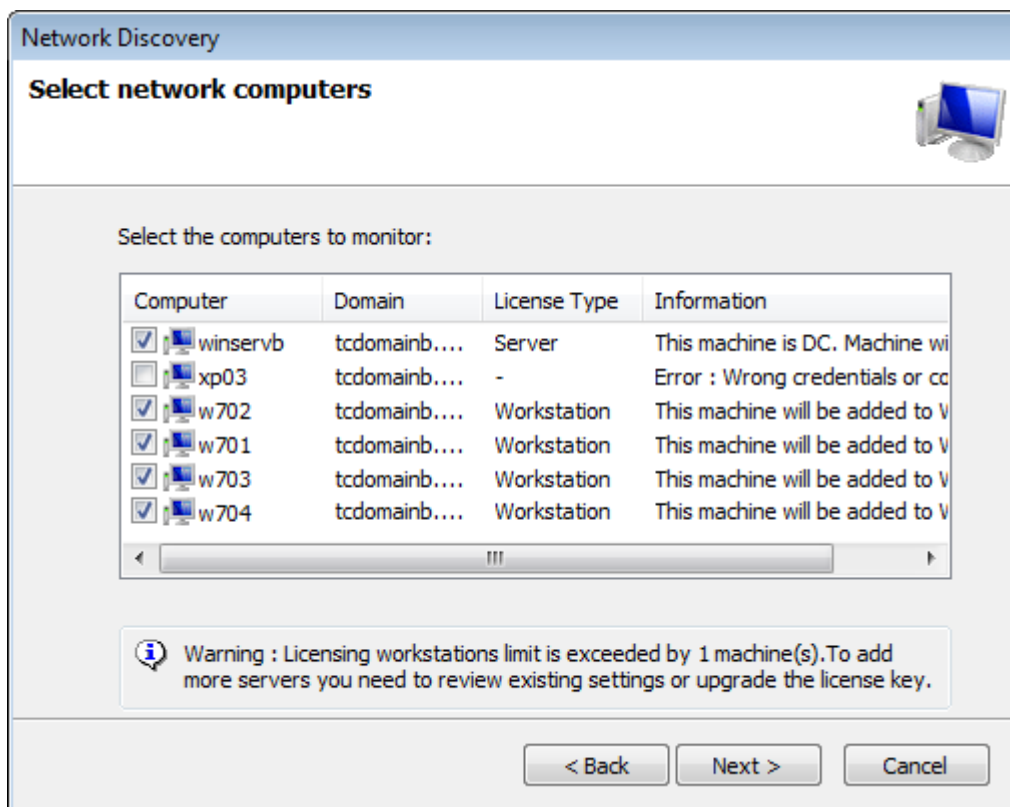
Screenshot 7 - Select the type of event source

3. The wizard enables you to search the local network for specific types of event sources. Select the type of event sources to add and click **Next**.



At least one event source type must be selected before proceeding to the next wizard dialog.

4. The wizard will automatically start to search for connected computers. On completion, click **Next**.



Screenshot 8 - Select computers from result



All discovered machines are selected by default. If the wizard fails to login to a computer, it is not selected.

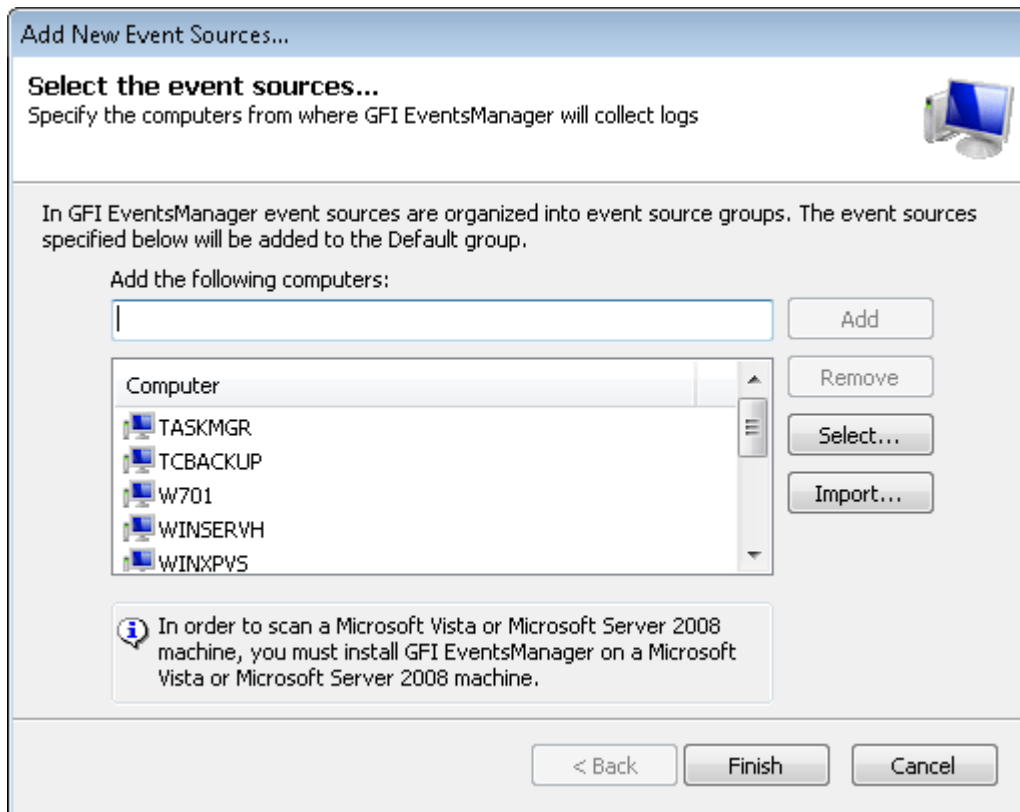
5. To add a computer not selected by default, click the respective computer and a dialog will enable you to key in alternative credentials.

6. Click **Next** and **Finish**.

Processing events from selected machines

To collect event logs from selected machines:

1. From the Quick Launch Console , click Process events - selected machines to launch the Add New Event Sources... wizard.



Screenshot 9 - Process events from selected machines

2. Specify the event source name or IP and click **Add**. Repeat until you have specified all the event sources to add to this group.

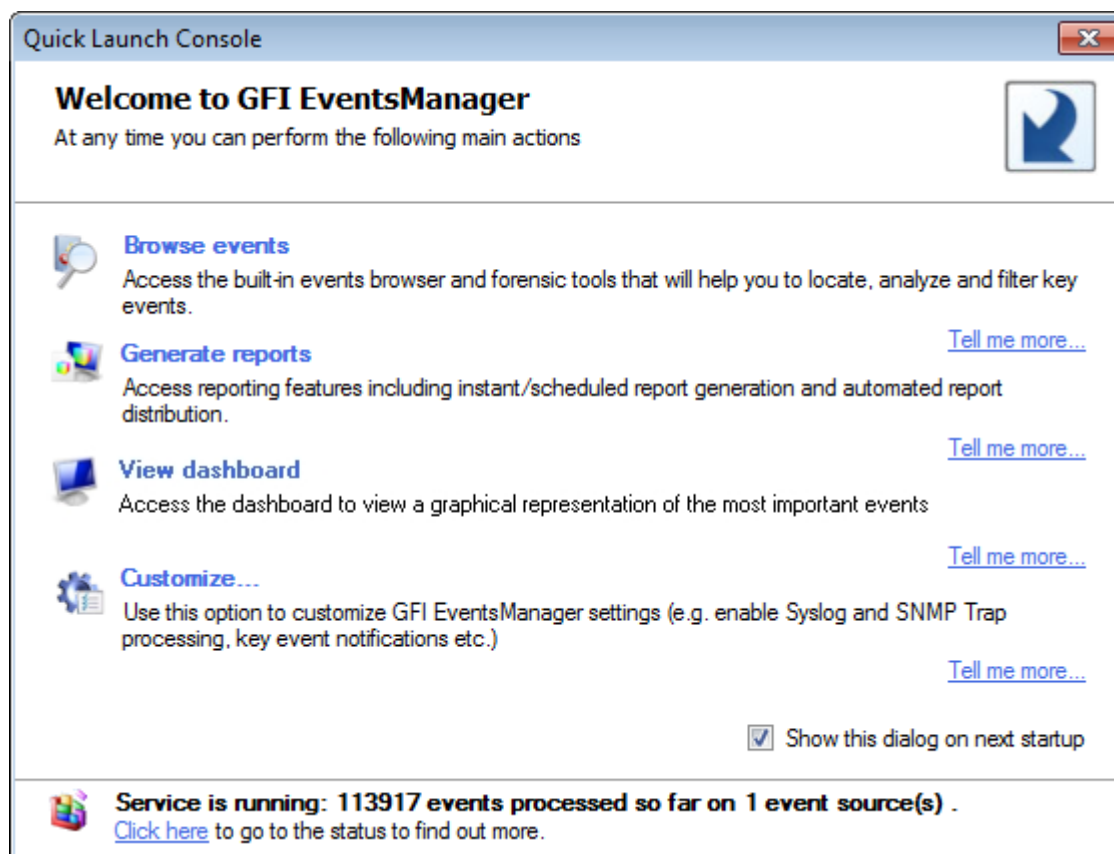


To import the list of event sources from a text file click **Import** button. To select event sources from a list, click **Select** button.

3. Click **Finish** to finalize settings. GFI EventsManager will collect events from the configured sources immediately.

3.8.2 Step 2: Analyze events and generate reports

After collecting the event logs, you can analyze the information and generate reports based on the gathered data.



Screenshot 10 - GFI EventsManager Quick Launch Console

To analyze events:






1. Click  [Open Quick Start Dialog](#) from the top right corner of the GFI EventsManager user interface. The table below describes the options available in the **Quick Launch Console**.

Table 11 - Quick Launch Console options

ICON	DESCRIPTION
	Browse events Access the built-in events and forensic tools that will help you to locate, analyze and filter key events. For more information refer to Event browsing chapter in this manual.
	Generate reports Access reporting features including instant/scheduled report generations and automated report distribution. For more information refer to Reporting chapter in this manual.
	View dashboard Access GFI EventsManager status dashboard. This enables you to view graphical representations of the most important events collected and processed by GFI EventsManager. For more information, refer to Status monitoring section in this manual.
	Customize Customize GFI EventsManager settings, such as enabling Syslog, SNMP Trap processing, key events notifications, and more. For more information refer to Manage event sources chapter in this manual.

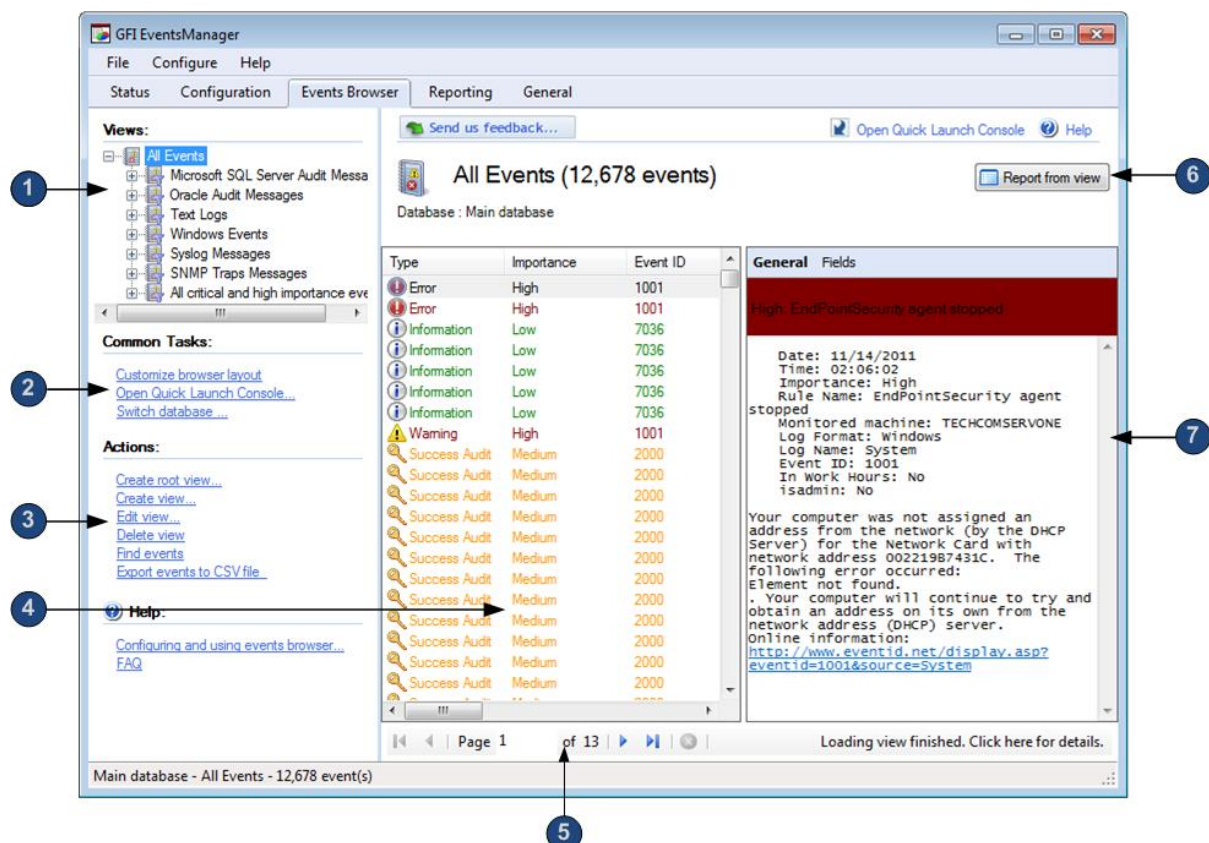
4 Event browsing

4.1 Introduction

The Event Browser enables you to access and browse processed or unprocessed event logs currently stored in the database. This chapter provides information about how to analyze events and contains the following sections:

- » Navigating through the Events Browser
- » Creating custom Root Views / Views
- » Event color-coding options
- » Event finder tool
- » Export to CSV tool
- » Rule finder tool
- » Reporting options
- » Switching database

4.2 Navigating the Events Browser



Screenshot 11 - Events Browser


The Events Browser is made up of the following sections:

Table 12 - Navigating the Events Browser

	SECTION	DESCRIPTION
1	Views	The Views section includes a wide range of predefined views. Use this section to view specific logs such as Windows Event Logs, W3C logs, SQL Server audits and more.
2	Common Tasks	Common Tasks enable you to customize the look of the Events Browser and switch database to view exported and/or archived event logs.

	SECTION	DESCRIPTION
3	Actions	Use the Actions section to run common functions related to analyzing event logs. This enables you create or edit custom views, export events for further analysis and more.
4	Events	The Events section is used to browse through the events categorized under the selected view (from section 1).
5	Navigation controls	Use the navigation controls to browse through collected events.
6	Reporting	The Report from view option enables you to generate graphical and statistical reports based on the selected view (from section 1).
7	Event Description Pane	<p>The Events Description Pane provides an extensive breakdown of the selected event (from section 4). Use this section to analyze the event details and find out when the event was generated, what was the cause and by whom it was generated. The header color coding enables you to quickly identify the severity of the event.</p> <p>The description section enables you to switch between two views:</p> <ul style="list-style-type: none"> » General - Contains event information in the legacy format that was standard for pre-Microsoft Windows Vista event logs. » Fields - Contains a list of event information categorized by fields.

Use the **Events Browser** for forensic analysis of events. All events accessible through the **Events Browser** are organized by log type in the **Views** section.

	<p>The link provided in the event description gives you access to:</p> <ul style="list-style-type: none"> » A more detailed description of the event » Information and links that explain what causes this type of event » Hints and tips on how to possibly solve any existing issues.
---	--

Event analysis is quite a demanding task; GFI EventsManager is equipped with specialized tools that simplify this process as well as enable the export of events. A description of these tools is provided in the following sections.

4.3 Creating custom Root Views / Views


In Events Browser, GFI EventsManager enables you to create two different types of custom views. The table below describes these views:

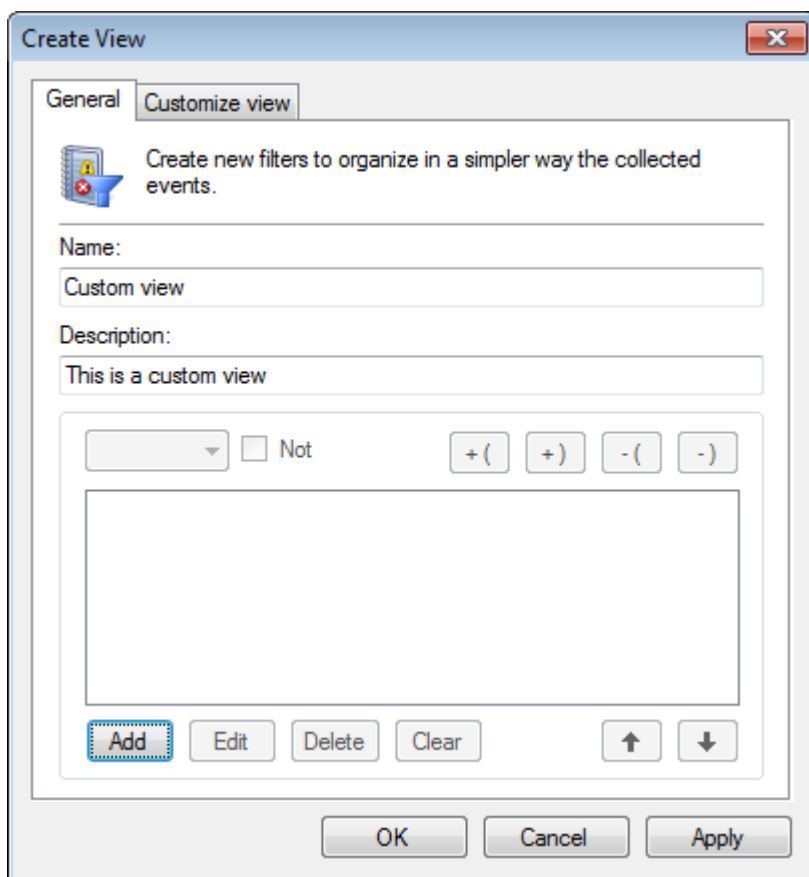
Table 13 - Event Browser: Create new view

VIEW TYPE	DESCRIPTION
Create root view...	Enables you to create top-level views which may contain a number of sub-views. This creates a new set of views beneath the ones that ship with the product (Example: All Events view).
Create view...	Create views within root views. Custom views can be added to the default root views and views.

To create a Root view/View:

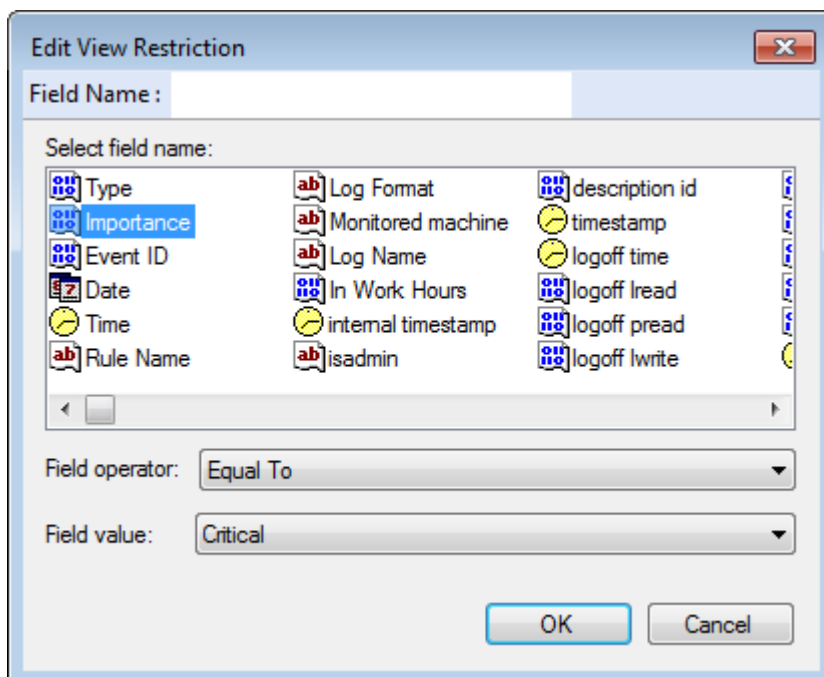
1. From Events Browser ► Actions, click Create root view.../Create view...

	Both options launch the same Create view dialog and are both configured in the same way. The difference is the positioning of the new custom view.
---	---



Screenshot 12- Custom view builder

2. Key in a name and description for the new view.
3. Click **Add** to add conditions to your view. If no conditions are specified, the view will display information from every event log type.

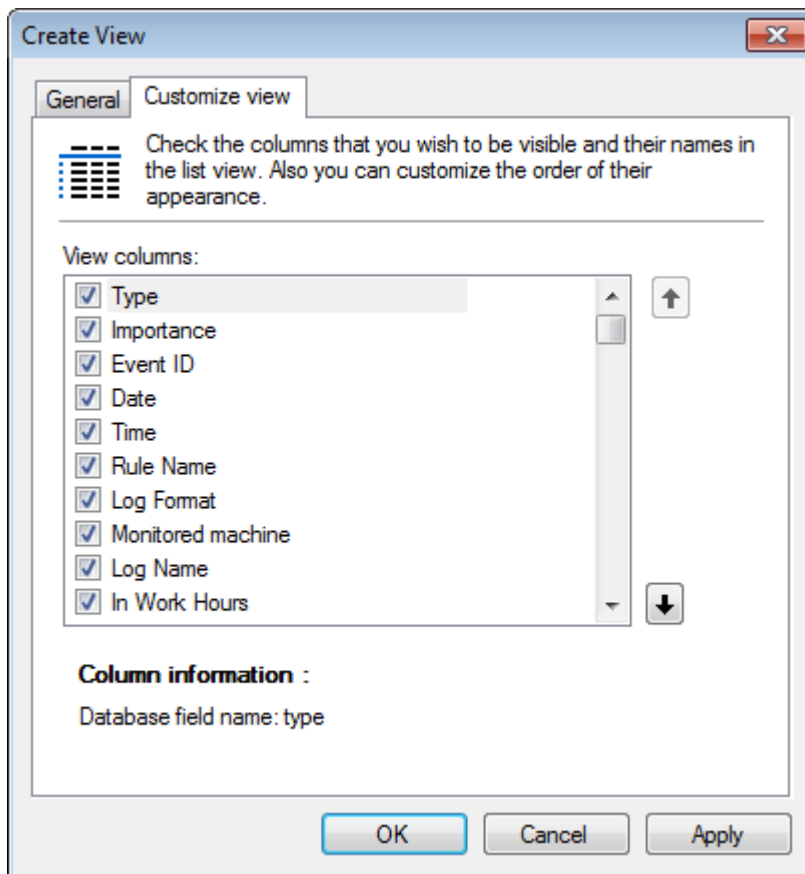


Screenshot 13- Edit view restriction

3. Select a field from the list of available fields and specify the **Field operator** and **Field value**. Click **OK**.

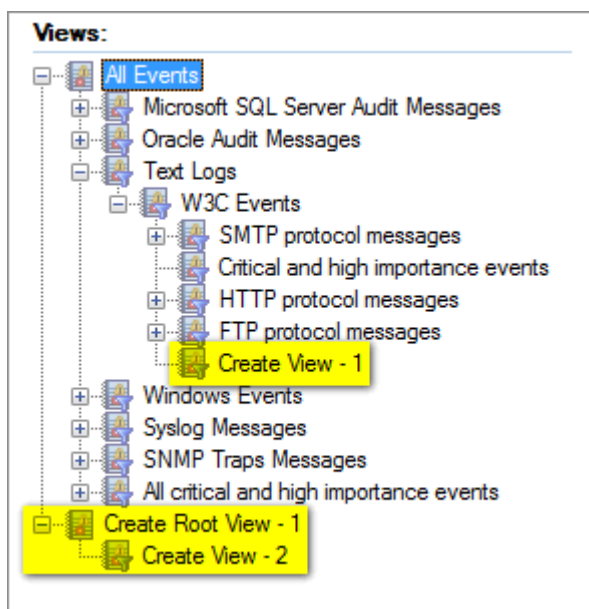


Repeat until all required query conditions are specified. For more information, refer to [Defining Restrictions](#).



Screenshot 14- Customize View tab

4. Click **Customize view** tab to select the columns to show in the new custom view. You can also arrange their order of appearance using the **Up** and **Down** arrow buttons.
5. Click **OK** to finalize your settings.



Screenshot 15 - Sample: New Root Views and Views

4.3.1 Deleting a view

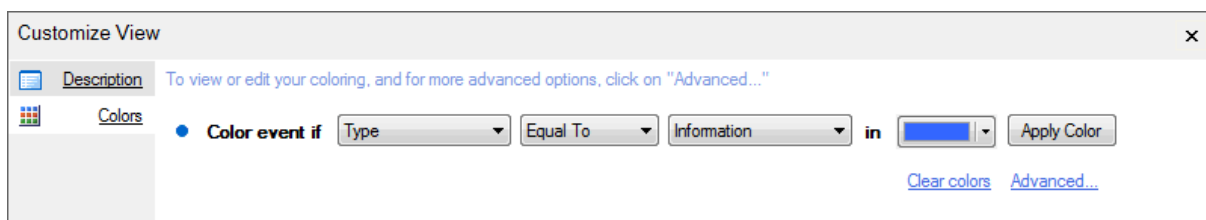
1. From **Events Browser ► Views**, select the view to delete.
2. Right-click on the view and click **Delete view**.

4.3.2 Editing a view

1. From **Events Browser ► Views**, select the view to edit.
2. From Actions click Edit view...
3. From the **View Properties** dialog, add, edit or delete conditions according to your requirements.

4.4 Event color-coding options

Use the event color-coding tool to tint key events in a particular color. This way the required events are easier to locate during event browsing.



Screenshot 16 - Color coding configuration

4.4.1 Assigning a color-code to a specific event

To assign a color code to a specific event:

1. From **Events Browser** select **Customize view ► Colors**.
2. Specify event filtering parameters including the color to be applied to the sifted events.
3. Click **Apply Color** button to save changes.

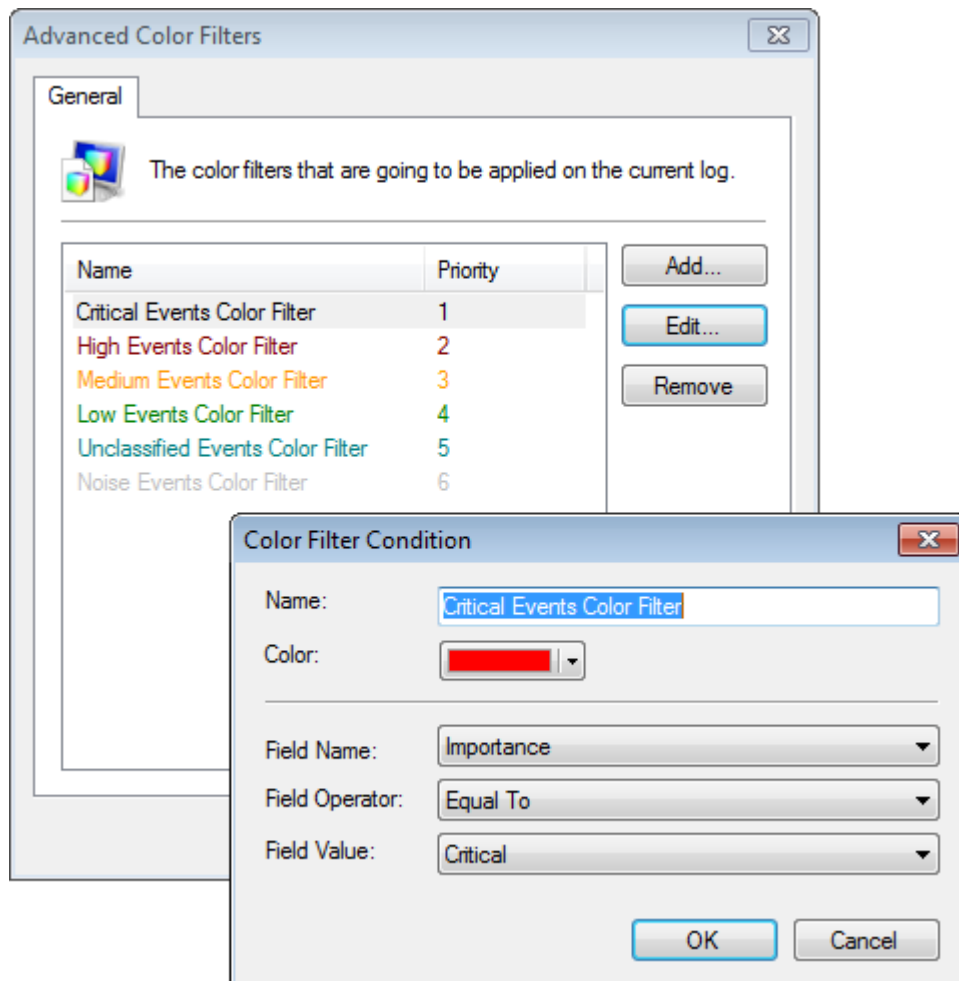


Use the **Clear color** option to clear all color settings.

4.4.2 Assigning different color-codes to multiple events

To assign different color-codes to multiple events:

1. From **Events Browser** select **Customize view ► Colors ► Advanced...**



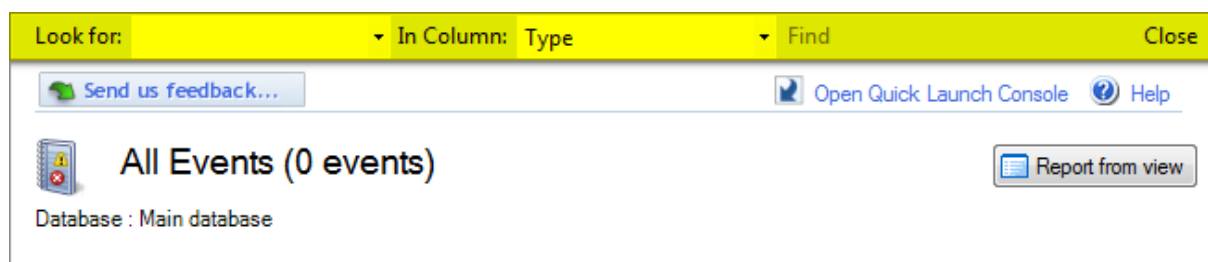
Screenshot 17 - Advanced Color Filter

3. Click **Add** button. Specify filter name and configure event filter parameters.
4. Click **OK** button to save filter settings.
5. Repeat until all required event filter conditions have been configured. Click **OK** to finalize your settings.

4.5 Event finder tool

Use the event finder tool to search and locate specific events using simple customizable filters. To search for a particular event:

1. Click Events Browser ► Actions ► Find events.



Screenshot 18 - Event finder tool

2. Configure the event search parameters through the options provided on top of the right pane. To trigger a case sensitive search, click **Options** and select **Match whole word**.
3. Click **Find** button to trigger the search.

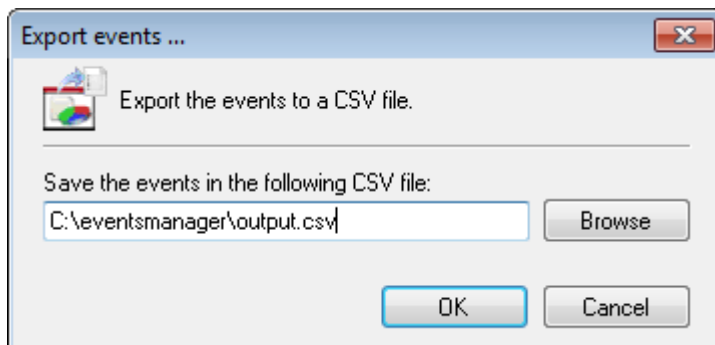
4.6 Export to CSV tool

GFI EventsManager enables you to export event data to CSV files directly from Events Browser. This is extremely convenient especially when further processing of event data is required. This includes:

- » Distribution of key event data via email
- » Running automated scripts that convert CSV exported events data to HTML for upload on web/company intranet
- » Generation of graphical management reports and statistical data using native tools such as Microsoft Excel
- » Generation of custom reports using third party applications
- » Interfacing events data with applications and scripts built in-house.

To export events to CSV:

1. From **Events Browser ► Views**, right-click a view and select **Export events**.



Screenshot 19 - Export events tool

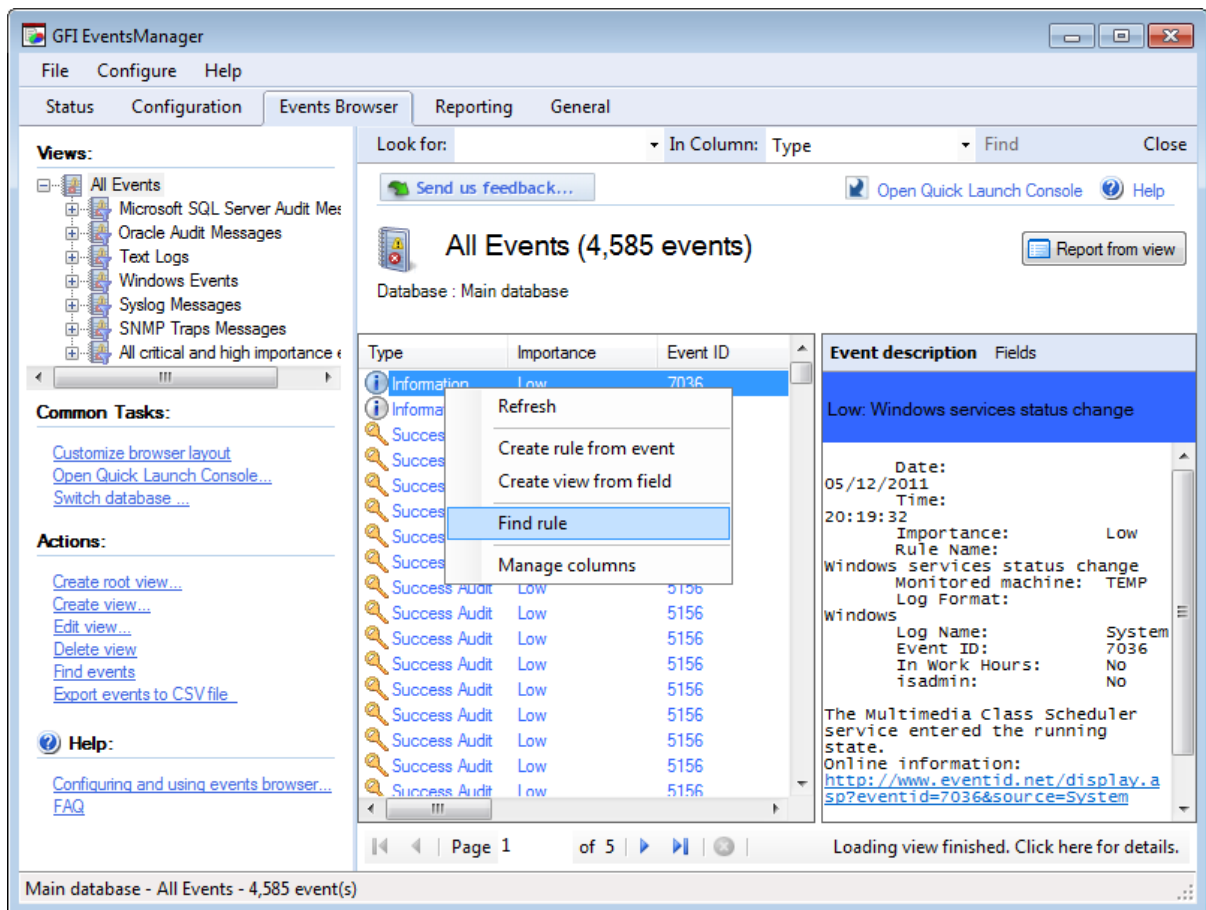
2. Specify or browse to where the exported events will be saved. Click **OK**.

4.7 Rule finder tool

GFI EventsManager enables you to find event processing rules from event logs in Events Browser.

To identify the rule(s) used for a specific event:

1. From **Events Browser**, right-click an event log.



Screenshot 20 - Find rule

2. Click **Find rule**.

4.8 Reporting options

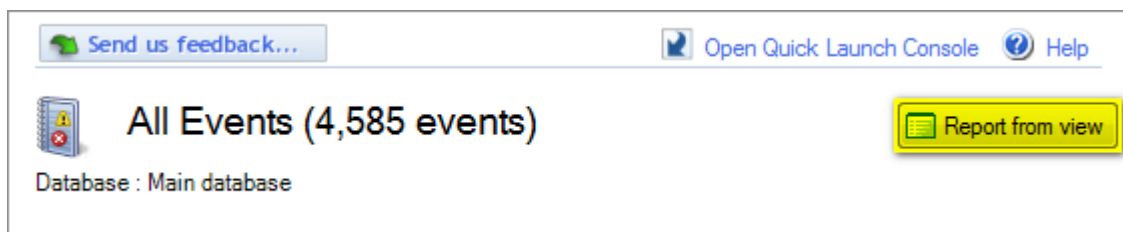
GFI EventsManager enables you to build your own a custom report (with graphs and statistics) based on a selected View from Events Browser.



GFI EventsManager ships a selection of predefined reports. We recommend that you check the available reports prior to creating new ones to avoid having duplicate reports.

To report from a view:

1. From **Events Browser ► Views**, select a view.



Screenshot 21 - Report from view button

2. Click **Report from view** from the top-right corner of the Events Browser.

3. From the **Create Report** dialog, configure the options from the tabs described below:

Table 14 - Event Browser: Create new report

TAB	DESCRIPTION
General	Specify the new report name and add conditions.
Layout	Select the columns that you want to be visible in the report. You can also customize the order of appearance.
Chart	Select Use graphical charts to generate a report showing information in a chart. The available chart types are: <ul style="list-style-type: none"> » Pie chart » Bar chart » Line graph.
Schedule	Select Use schedule to enable report scheduling. Configure the generation date and frequency for the new report.



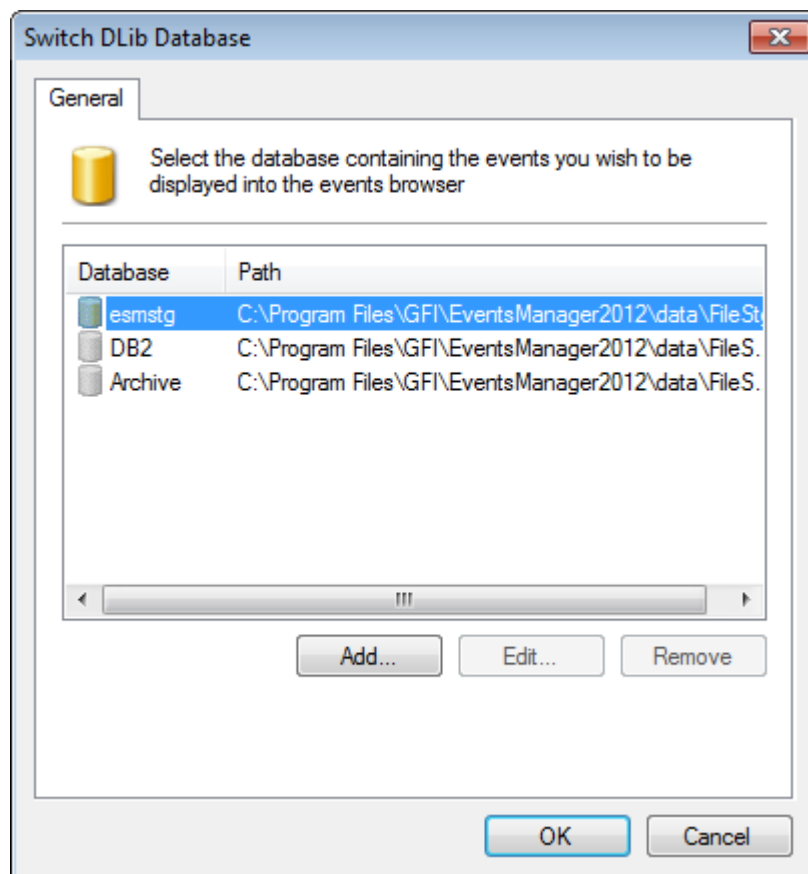
For more information, refer to [Creating custom reports](#).

4.9 Switching database

For event browsing purposes, GFI EventsManager enables you to switch between different databases. Use this feature to browse events that have been exported or archived for further analysis.

To switch database:

1. Click Events Browser ► Common Tasks ► Switch database.



Screenshot 22 - Switch database dialog

2. Select the database from the list of databases and click **OK**.



You can click **Add...** to specify a path and database name. Click **Edit...** to edit the specified information.

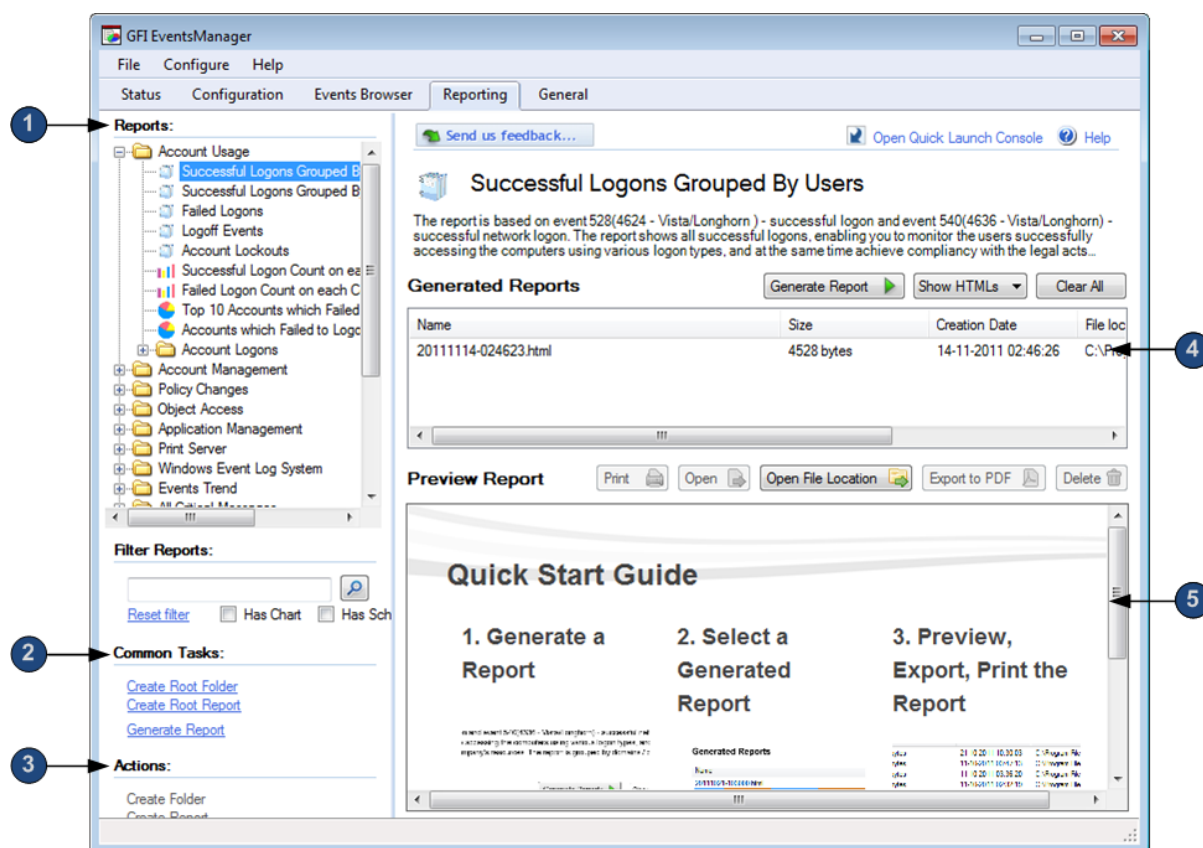
5 Reporting

5.1 Introduction

GFI EventsManager provides a fully-fledged reporting system. It ships with a number of reports including technical and executive level reports showing graphical and statistical information based on hardware and software audited by GFI EventsManager. This chapter contains the following sections:

- » Navigating the Reports tab
- » Available reports
- » Managing reports
- » Generating reports
- » Analyzing reports
- » Creating custom reports

5.2 Navigating the Reports tab



Screenshot 23 - Navigating the Reporting UI

The Reporting tab consists of the sections described below:

Table 15 - Navigating the Reporting tab

SECTION	DESCRIPTION
1	The Reports section contains all the predefined reports that ship with the product. Use this section to organize and generate various reports from technical to executive type.
2	The Common Tasks section enables you to quickly launch typical operations such as creating folder and report views to organize reports and generating reports.
3	From the Actions sections, you are able to create, edit or delete reports according to your needs.

SECTION	DESCRIPTION
4	Use the Generated Reports section to view the history of a selected report (from Section 1). This enables you to regenerate the report and export the report to HTML and/or PDF.
5	The Preview Report section provides a view of a selected, generated report. Use the control buttons to Print, Open, Export or Delete reports directly from this section.

5.3 Available reports

GFI EventsManager's extensive report list contains reports for various requirements designed to facilitate reporting as much as possible. The following report categories are included in GFI EventsManager by default. Each category contains a number of reports that can be used out of the box or customized to fit your requirements:

Table 16 - Available reports

REPORT CATEGORY	DESCRIPTION
Account Usage	Use the reports in this category to identify user logon issues. The event details shown in these reports include successful/failed user logons and locked user accounts.
Account Management	Use the reports in this category to generate a graphical overview of important events that took place across your entire network. The event details shown in these reports include changes in user and computer accounts as well as changes in security group policies.
Policy Changes	Use the reports in this category to identify policy changes effected on your network.
Object Access	Use the reports in this category to identify object access issues. The event details shown in these reports include successful/failed object access and objects that have been deleted.
Application Management	Use the reports in this category to identify faulty applications and application installation and removal issues. The event details shown in these reports include applications that have been installed or removed as well as applications, which are crashing and hanging.
Print Server	Use the reports in this category to display details related to printing events. Details provided in these reports include documents that have been printed, the users that triggered the printing event and the date/time when the printing operation took place.
Windows Event Log System	Use the reports in this category to identify audit failures and important Windows event log issues. Details provided in these reports include the starting and stopping of event log services, clear log operations as well as errors generated during event logging.
Events Trend	Use the reports in this category to display statistical information related to event generation. Charts provided enumerate the 10 computers and users with most events. Other reports provide event counts on a network-wide basis as well as on a computer-by-computer basis. Reports in this category can be generated for each main time - by hour, day, week or month.
All Critical	Use the reports in this category to display information related to critical Windows events, Syslog, W3C, Custom Events, SNMP Traps and SQL Server Audit events. The charts provided enumerate the 10 most critical events.
Miscellaneous, Customizable	Use the reports in this category to generate reports that offer broad customization. These can be used to generate reports based on any Windows event log, using filtering conditions and grouping modes that are not covered by the other default reports.
PCI DSS Compliance / GCSx Code of Connection Requirements / SOX Compliance / HIPAA Compliance / GLBA Compliance	Use the reports in these categories to generate legal compliance regulations reports.
General and Security Requirements	Use the reports in this category to generate various reports required by several GCSx Code of Connection memos.
LOGbinder SP reports	Use the reports in this category to generate reports related to Microsoft SharePoint audit events.

5.4 Managing reports

Reports are organized in a tree structure enabling you to easily find and generate the required report. GFI EventsManager includes three options that allow you to maintain the report structure as the number of reports increase by time. These options include:

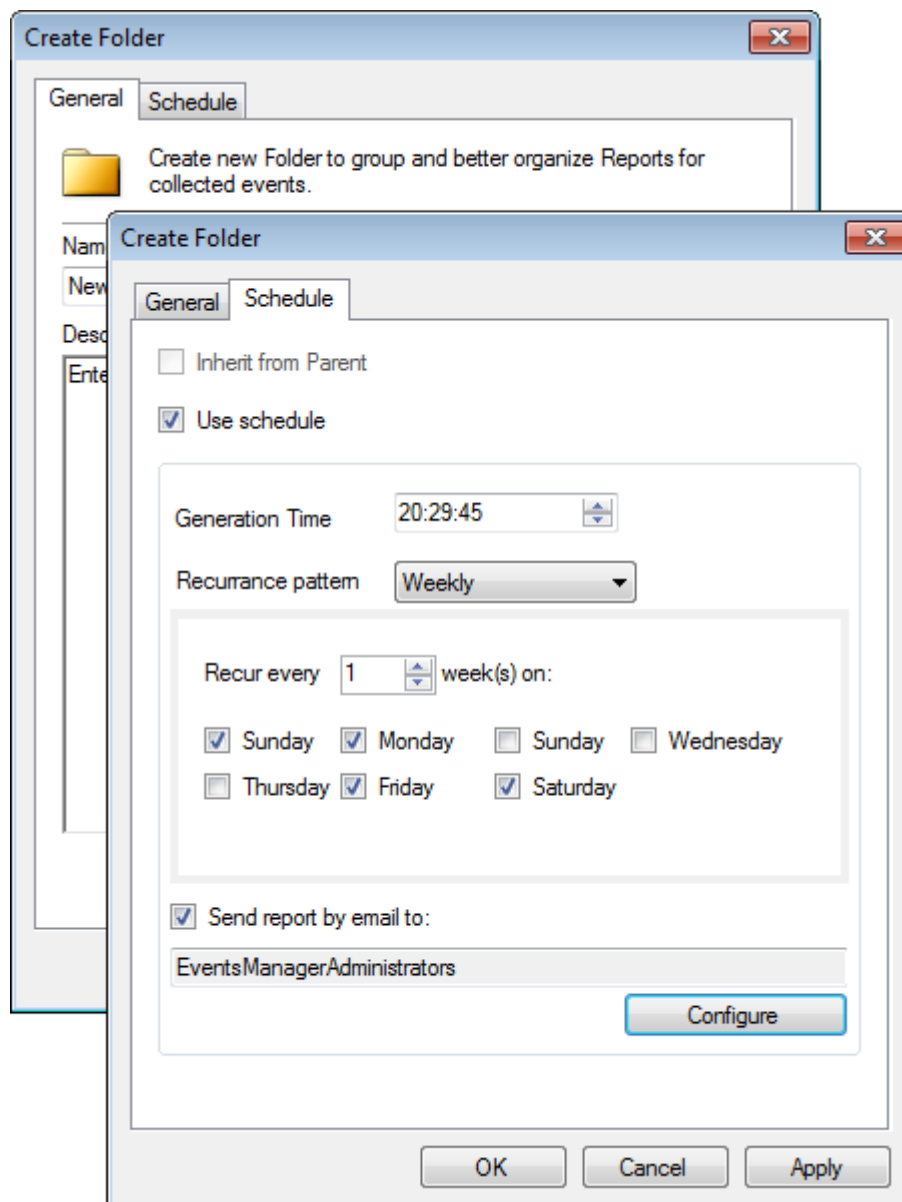
Table 17 - Managing reports

OPTION	DESCRIPTION
Create Root Folder	Create top-level folders that may contain one or more subfolders or reports. For more information, refer to Creating a root folder .
Create Folder	Create a folder within a root folder. Folders may contain any number of reports. For more information, refer to Creating a folder .
Create Root Report	<p>Root reports behave in the same way as root folders. These are created at the top level and may contain a number of sub reports. For more information, refer to Creating a root report.</p> <p>Example: You can create a root report which is generated once every month. Then you can create daily reports covering specific topics of the root report, generated on daily basis.</p>

5.4.1 Creating a root folder

To create a root folder:

1. From Reporting tab ► Common Tasks, click Create Root Folder.



Screenshot 24 - Create Report Folder dialog

2. From the **General** tab, specify a name and a description (optional) for the new folder.
3. (Optional) Click **Schedule** tab and select **Use schedule** to configure a schedule for the reports included in this new folder. Configure the options described below:

Table 18 - Create folder: Schedule options

OPTION	DESCRIPTION
Inherit from Parent	Select when the new folder is part of a root folder that already has scheduling configured.
Use schedule	Select Use Schedule to enable scheduling of the reports contained in the new folder.
Generation time	Specify the time when reports are generated.
Recurrence pattern	Specify the report generation frequency. Select from Daily , Weekly or Monthly pattern and configure the respective parameters.
Send report by email to	Select this option to enable email notifications. Click Configure to select the users from the Select users and groups... dialog. NOTE: Configure alerting options before using this feature. For more information, refer to Configuring Alerting Options .

4. Click **OK** to save your settings.

5.4.2 Creating a folder

To create a folder:

1. From **Reporting** tab ► **Reports**, right-click a root or sub folder and select **Create Folder**.
2. From the **General** tab, specify the name and description (optional) for the new group.
3. (Optional) Click **Schedule** tab and configure the required parameters.
4. Click **OK** to save your settings.

5.4.3 Creating root reports

To create a root report:

1. From **Reporting** tab ► **Common Tasks**, click **Create Root Report**.
2. From **General** tab, specify a name and description (optional) for the new root report.
3. Click **Add** to add conditions to your new report. For more information, refer to [Defining Report Restrictions](#).



Repeat this step until all required conditions have been specified.

4. Click **Layout** tab and add the column headings that you want to be visible in the report. For more information, refer to [Defining Column Headings](#).



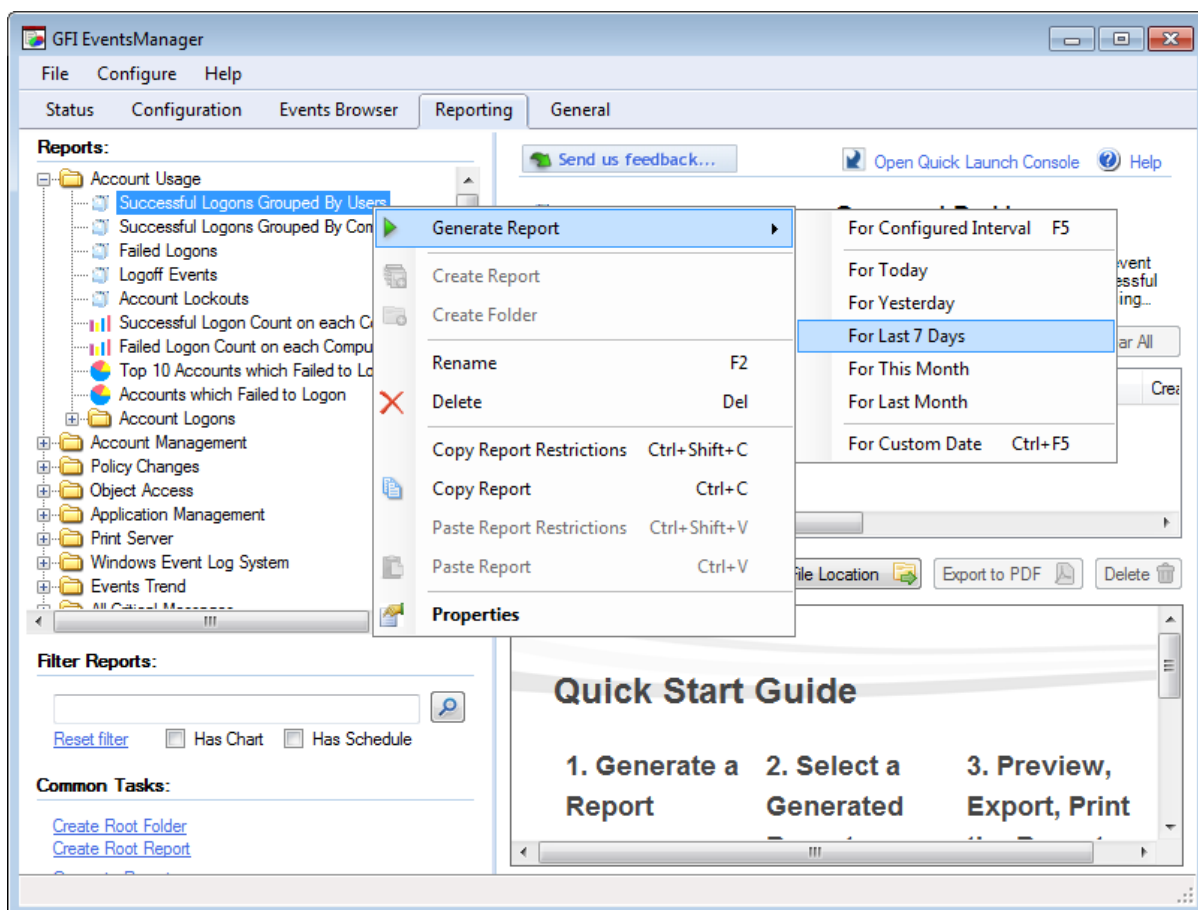
If you have a saved report template, click **Open location**, to browse and load your template.

5. (Optional) Click **Chart** tab and select **Use graphical charts** to include graphs in your report.
6. From the **Place chart at** drop-down menu, specify the location of the chart. Select from:
 - » Beginning of Report
 - » End of Report.
7. From **Properties** ► **X axis** and **Y axis**, configure the X and Y Axis properties.

8. (Optional) Click **Schedule** tab and configure schedule settings.
9. Click **OK** to save settings.

5.5 Generating reports

To generate a report:



Screenshot 25 - Generating a report

1. From **Reporting** tab ► **Reports**, right-click a report and select **Generate Report**.
2. Wait for the report to generate and view results in **Preview Report** section.



Reports can also be generated by selecting a report from the list and clicking **Generate Report** at the top of the reporting page.

GFI EventsManager™
 Event log monitoring, management and archiving

Successful Logons Grouped By Users

Found 103 matching records.

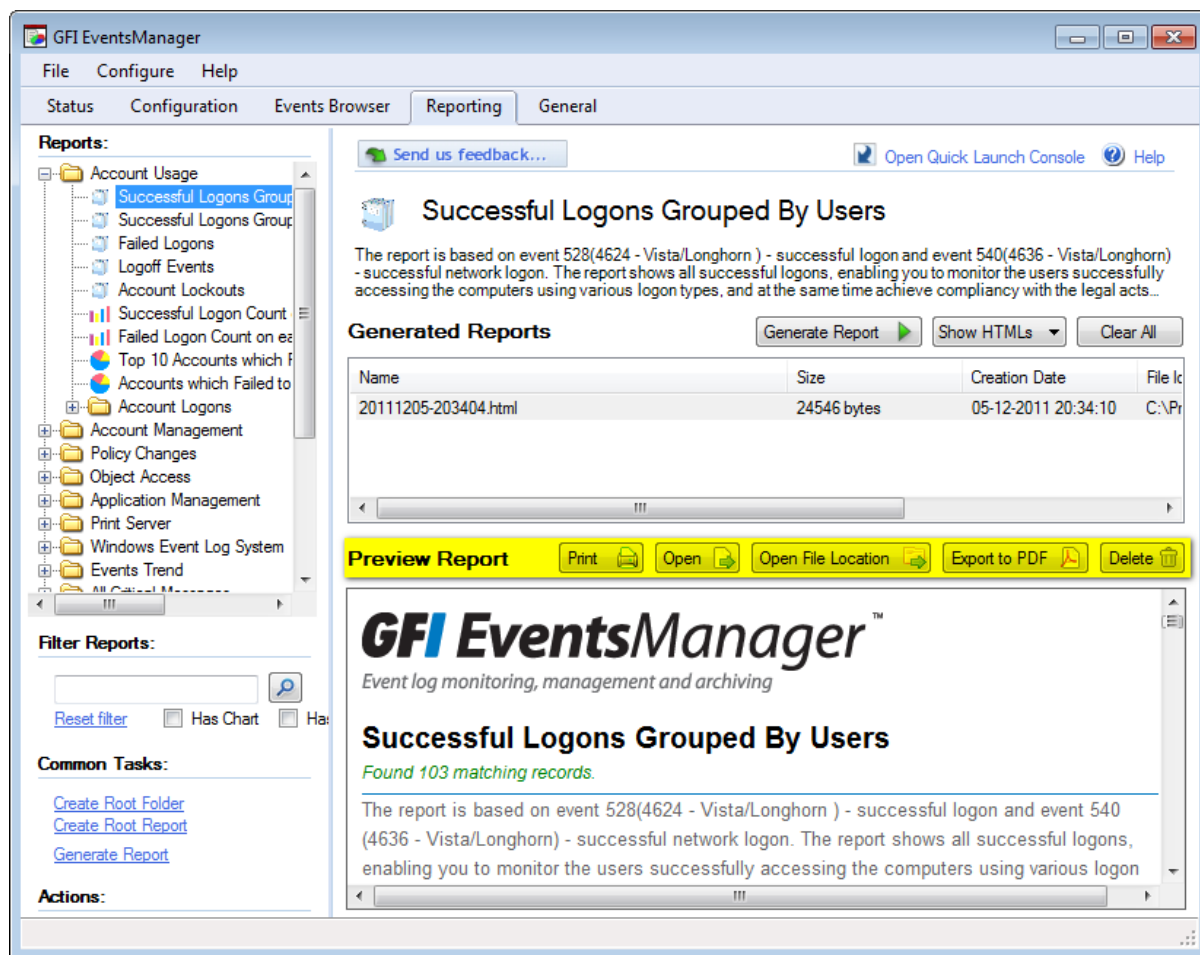
The report is based on event 528(4624 - Vista/Longhorn) - successful logon and event 540(4636 - Vista/Longhorn) - successful network logon. The report shows all successful logons, enabling you to monitor the users successfully accessing the computers using various logon types, and at the same time achieve compliance with the legal acts which require monitoring of access to the company's resources. The report is grouped by users thus providing a quick view of the computers used by each user.

User Name: John Smith

Computer	Event ID	Description	Account	Logon Type	Time	Date
TEMP	4624	An account was successfully logged on.	ANONYMOUS LOGON	Network	20:09:05	2011-12-05
TEMP	4624	An account was successfully logged on.	John Smith	Network	20:11:21	2011-12-05
TEMP	4624	An account was successfully logged on.	John Smith	Network	20:11:21	2011-12-05

Screenshot 26 - Report sample

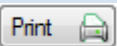
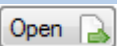
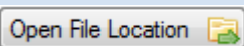
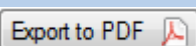

5.6 Analyzing reports



Screenshot 27 - Preview Report: Analyzing

The reporting system of GFI EventsManager comes with dedicated tools to help you analyze and export reports. Once a report is generated, select it from the list of **Generated Reports** and use the common controls which help you run common report analysis commands. The available tools are described below:

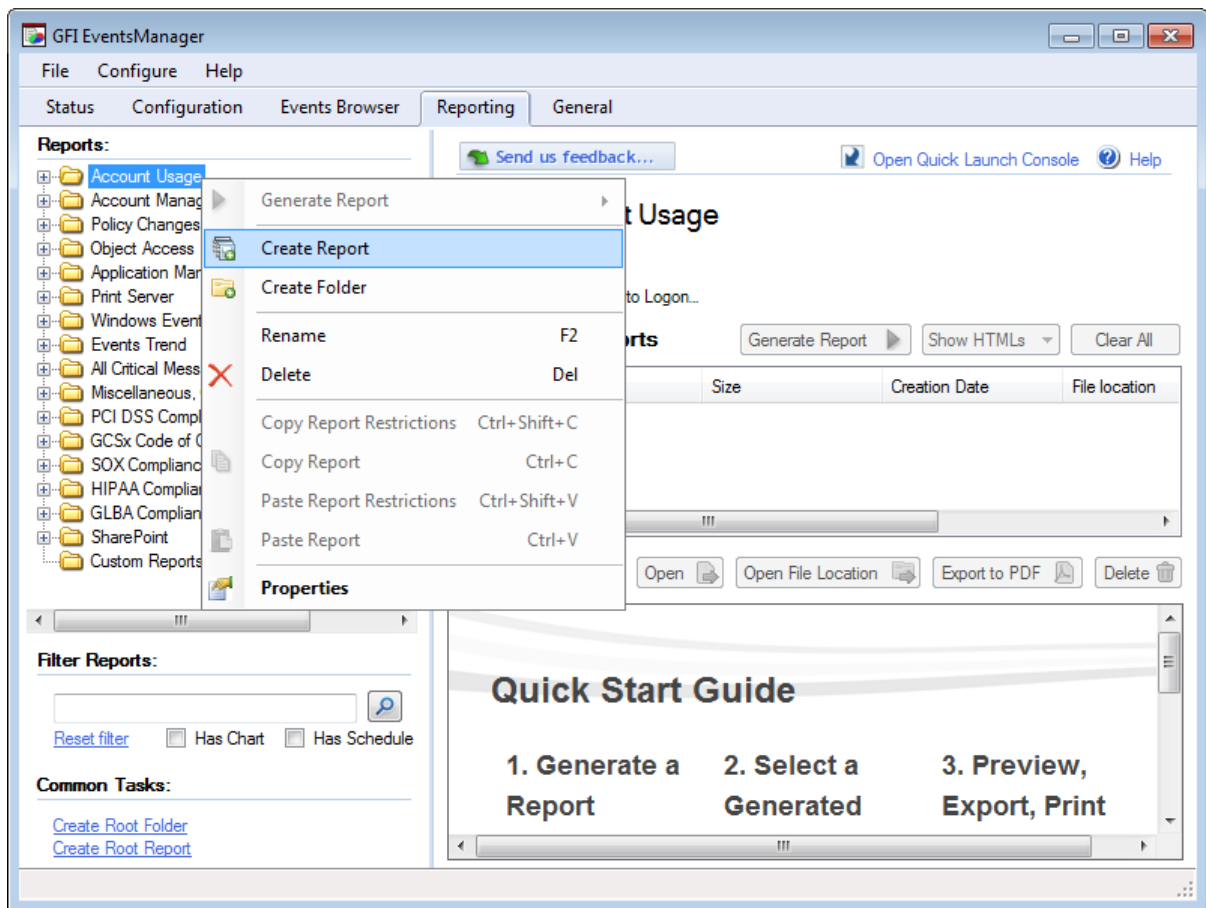
Table 19 - Analyzing reports tools

OPTION	DESCRIPTION
	Use the Print option to view a print preview, configure printer settings and print the selected report.
	Use the Open button to open the selected report in a browser. GFI EventsManager uses your default browser to view reports in HTML.
	The Open File Location button enables you access the folder containing the report for backup or archiving purposes.
	Use Export to PDF to export the selected report to Portable Document Format.
	Click Delete to remove a generated report from the list.

5.7 Creating custom reports

Creating custom reports requires attention while setting up conditions. Conditions are set to determine what is filtered and presented in the report. Failing to configure conditions properly generates unwanted noise and inaccurate information.

To create a new custom report:



Screenshot 28 - Creating a new report

1. From Reporting tab ► Reports, right-click a root folder/folder/root report and select Create Report.

Screenshot 29 - Creating a report: General

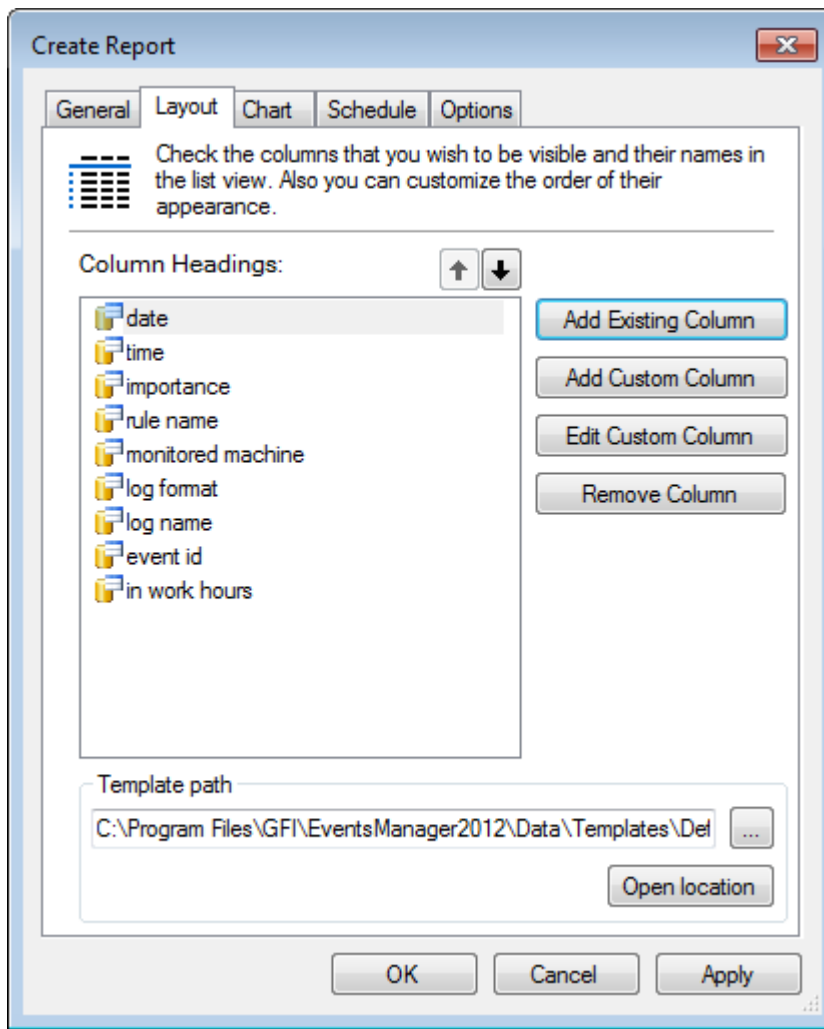
2. From **General** tab, configure the options described below:

Table 20 - Create Report dialog: General options

OPTION	DESCRIPTION
Name	Enter a name for the new report.
Description	Optionally, enter a report description.
Select sort column	Specify sorting column name.
Ascending	Select Ascending to sort you report content from A to Z (as opposed to Z to A).
Add/ Edit / Delete / Clear	Use buttons to configure your report conditions. For more information, refer to Defining Restrictions .

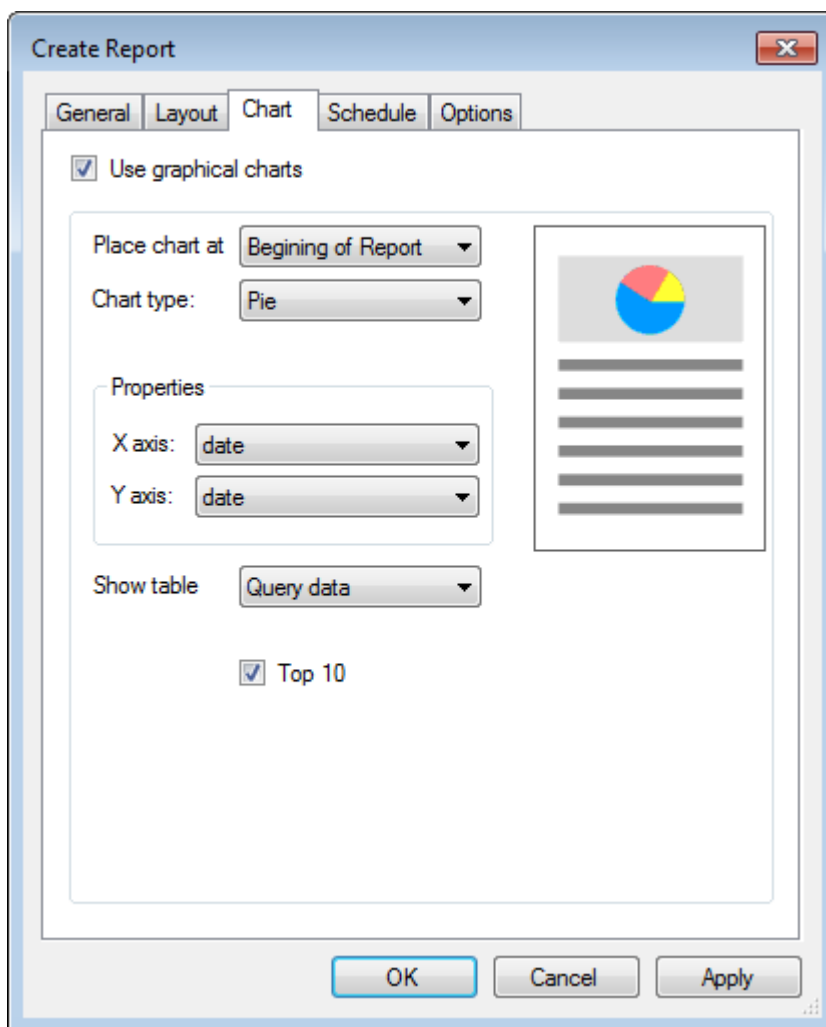


Copy report restrictions from existing reports from **Reporting** tab ► **Reports**. Right-click a report and select **Copy Report Restrictions**.



Screenshot 30 - Creating a report: Layout

3. Click **Layout** to add column headings that you want to be visible in your report. Use the **Up** and **Down** arrow buttons to arrange the order of their appearance. For more information, refer to [Defining Column Headings](#).

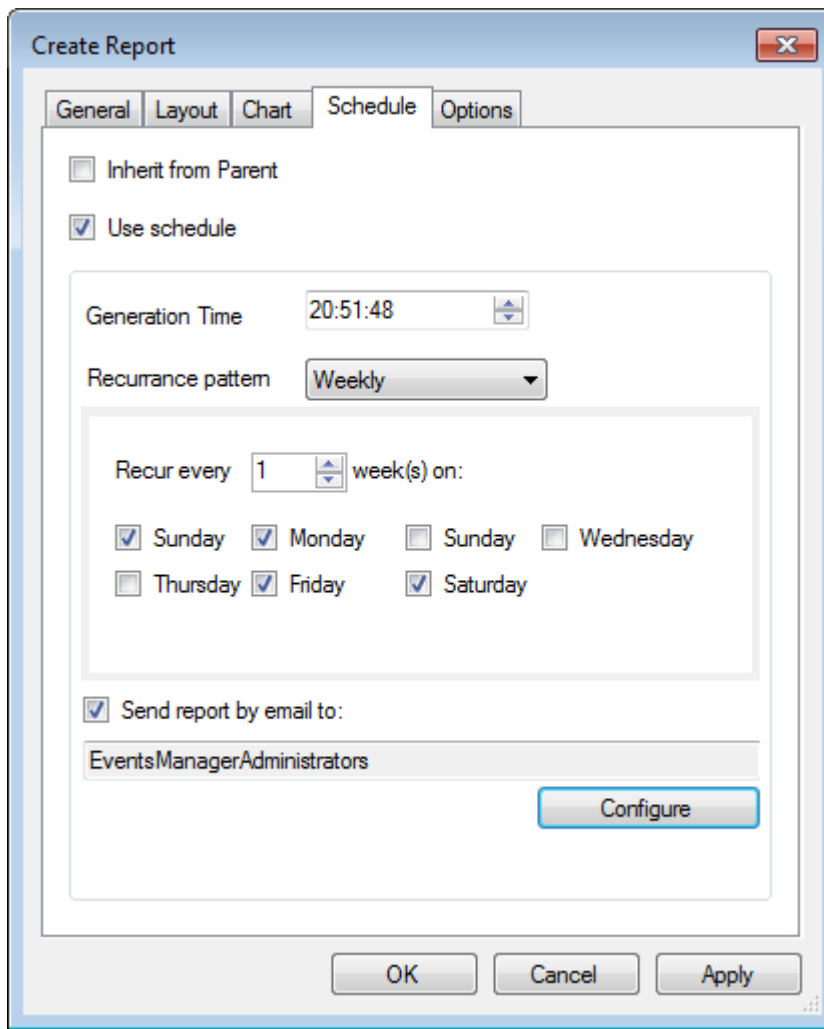


Screenshot 31 - Creating a report: Chart

4. (Optional) Click **Chart** tab and configure the options described below:

Table 21 - Create Report dialog: Chart options

OPTION	DESCRIPTION
Use graphical charts	Include a graphical chart to present your data as well as a text-based table.
Place chart at	Select between Beginning of Report and End of Report to place the chart at the selected location.
Chart type	Use the Chart type drop-down menu to select the type of chart to include in your report. Select from: <ul style="list-style-type: none"> » Pie chart » Bar chart » Line chart.
Properties	Select the information to display in the X and Y axis. The available options are the column headings selected in Step 3 .
Chart data	This is the data used to construct the chart. It is a smaller table that contains counts and grouped data useful for charting.

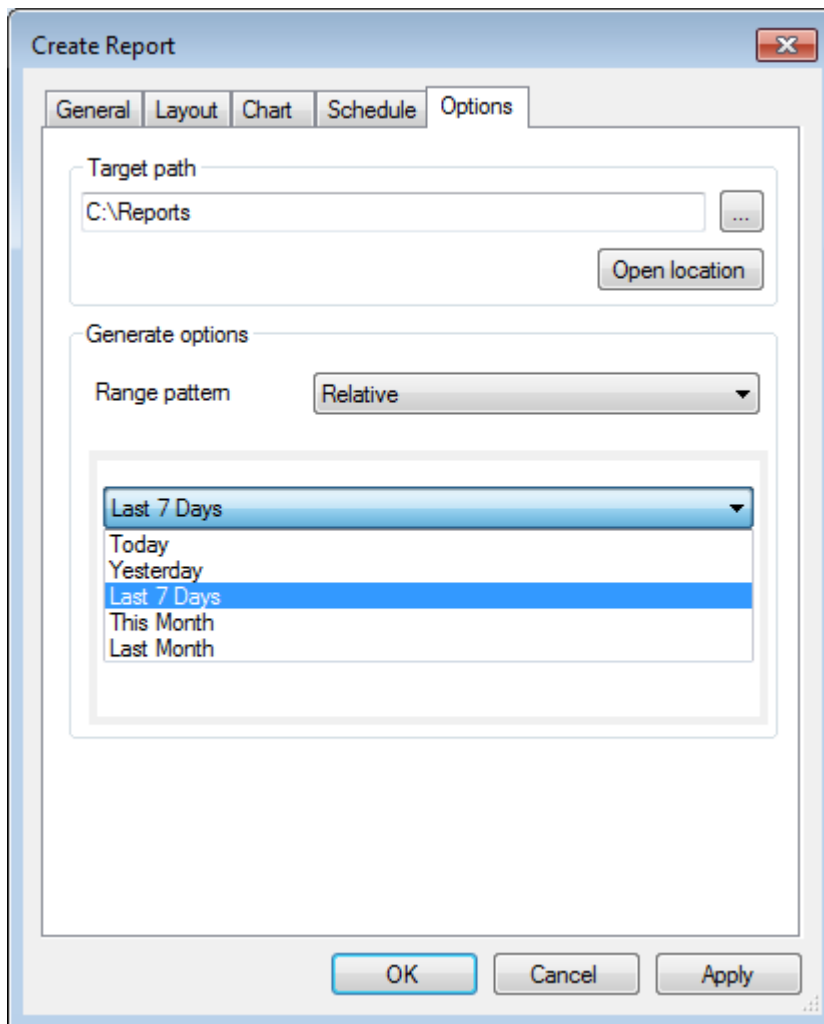


Screenshot 32 - Creating a report: Schedule

5. Click **Schedule** tab and configure the options described below:

Table 22 - Create Report dialog: Schedule options

OPTION	DESCRIPTION
Inherit from Parent	Select this option when the new folder is part of a root folder that already has scheduling configured.
Use schedule	Select Use Schedule to enable scheduling of the reports contained in the new folder.
Generation time	Specify the time when reports are generated.
Recurrence pattern	Specify the frequency of when the report is generated. Select from Daily, Weekly or Monthly pattern and configure the respective parameters.
Send report by email to	Select this option to enable email notifications. Click Configure to select the users from the Select users and groups... dialog. NOTE: Configure alerting options before using this feature. For more information, refer to Configuring Alerting Options .

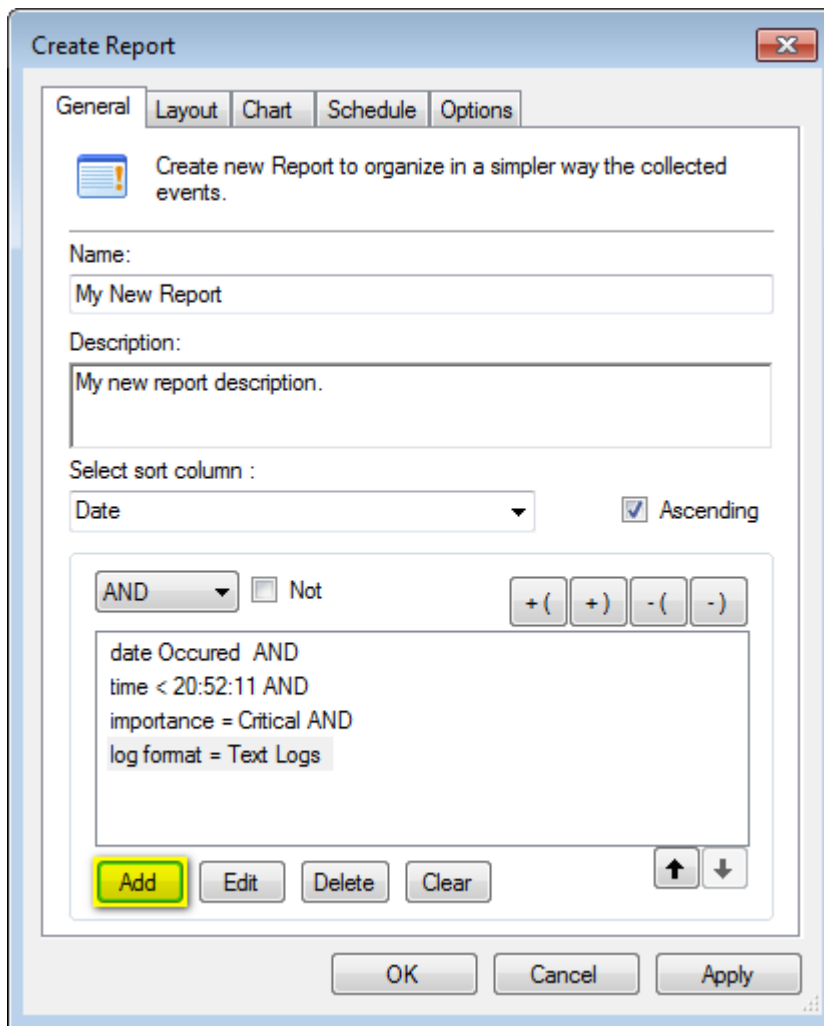


Screenshot 33 - Creating a report: Options

6. Click **Options** tab. From **Target path**, specify destination path where the new report is saved when it is generated.
7. From **Generate options** ► **Range pattern**, select the relevant pattern from which data is used to generate the new report.
8. Click **OK** to save your settings.

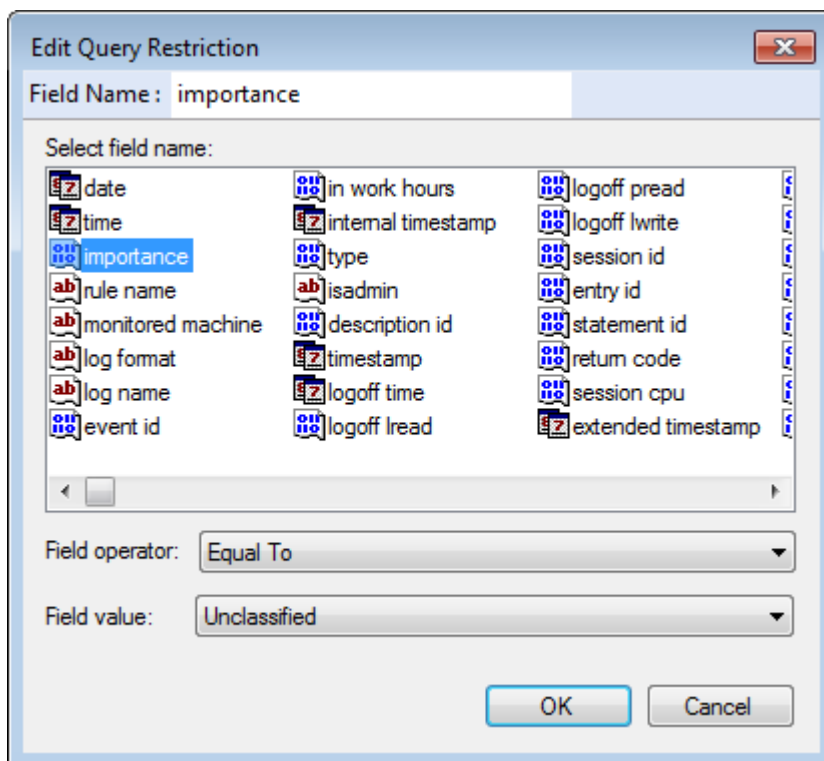
5.7.1 Defining Restrictions

Report restrictions are used to define what is filtered and presented in your reports. To configure conditions:



Screenshot 34 - Creating a report: Adding conditions

1. From the **Create View/Create Report** dialog, click **Add** to launch the **Edit Query Restriction** dialog.



Screenshot 35 - Creating a report: Edit Query Conditions

2. From the list of available fields, select a field.



Optionally, you can key in the name in the **Field Name** text box to search for the required field.

3. Specify a **Field Operator** for the selected field. Available operators include:

Table 23 - Defining restrictions: Field Operators

FIELD OPERATOR	DESCRIPTION
Equal To	When the event field is equal to the value configured.
Less than	When the event field is has a smaller value than the value configured.
Greater than	When the event field is has a larger value than the value configured.
Occurred (Related to date/time fields)	When the event field date occurred before the value date.
Like	When the event field has similar text as the value text.
Contains	When the event field contains the value text.
Value in List	When the event field is equal to one of the values in a list.

4. Specify a **Field Value** for the selected field and field operator. Some fields have predefined values while others require you to specify a value.

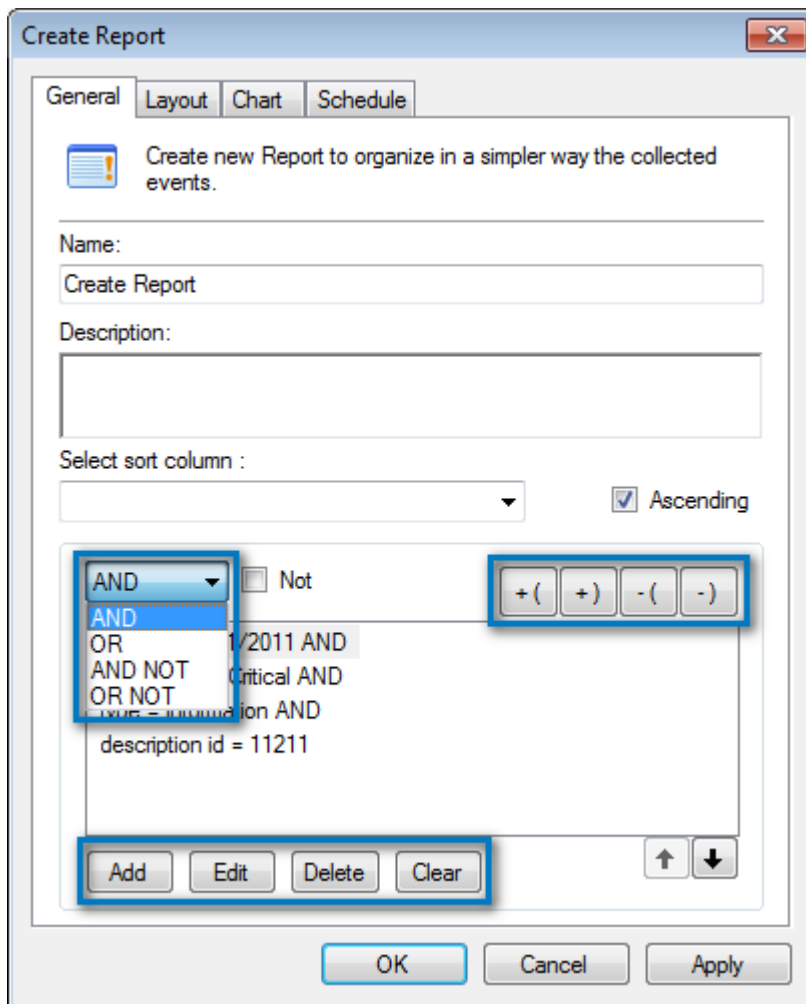
5. Click **OK** to save your restriction.



Copy report restrictions from existing reports from **Reporting** tab ► **Reports**. Right-click a report and select **Copy Report Restrictions**.



Repeat this step until all your restrictions are defined.



Screenshot 36 - Customizing the condition

6. Once all the restrictions are defined, use the options described below to customize the condition to further suite your requirements:

Table 24 - Defining restrictions: Query Condition tools

OPTION	DESCRIPTION
AND	Select the condition to configure and select AND . The selected condition AND the following condition(s) must be met for the query to be valid.
OR	Select the condition to configure and select OR . The selected condition OR the following condition(s) must be met for the query to be valid.
AND NOT	Select the condition to configure and select AND NOT . This means that the selected condition has to match the restriction parameters but the following conditions must not.
OR NOT	Select the condition to configure and select OR NOT . This means that the selected condition has to match the restriction parameters OR the following conditions must not.
+ (Click '+' ('(' to add an opening bracket to the selected condition. Conditions enclosed in brackets are processed first.
+)	Click '+' ')' to add a closing bracket to the selected condition. Conditions enclosed in brackets are processed first.
- (Click '-' ('(' to remove an opening bracket from the selected condition.
-)	Click '-' ')' to remove a closing bracket from the selected condition.
Add	Click Add to launch the restrictions dialog and add more fields to the condition.
Edit	Click Edit to access the restrictions dialog and customize the selected condition.
Delete	Click Delete to delete a condition.
Clear	The Clear button deletes all the query conditions.

OPTION	DESCRIPTION
Up arrow	Use the Up arrow key to move the selected condition up in the list.
Down arrow	Use the Down arrow key to move the selected condition down in the list.

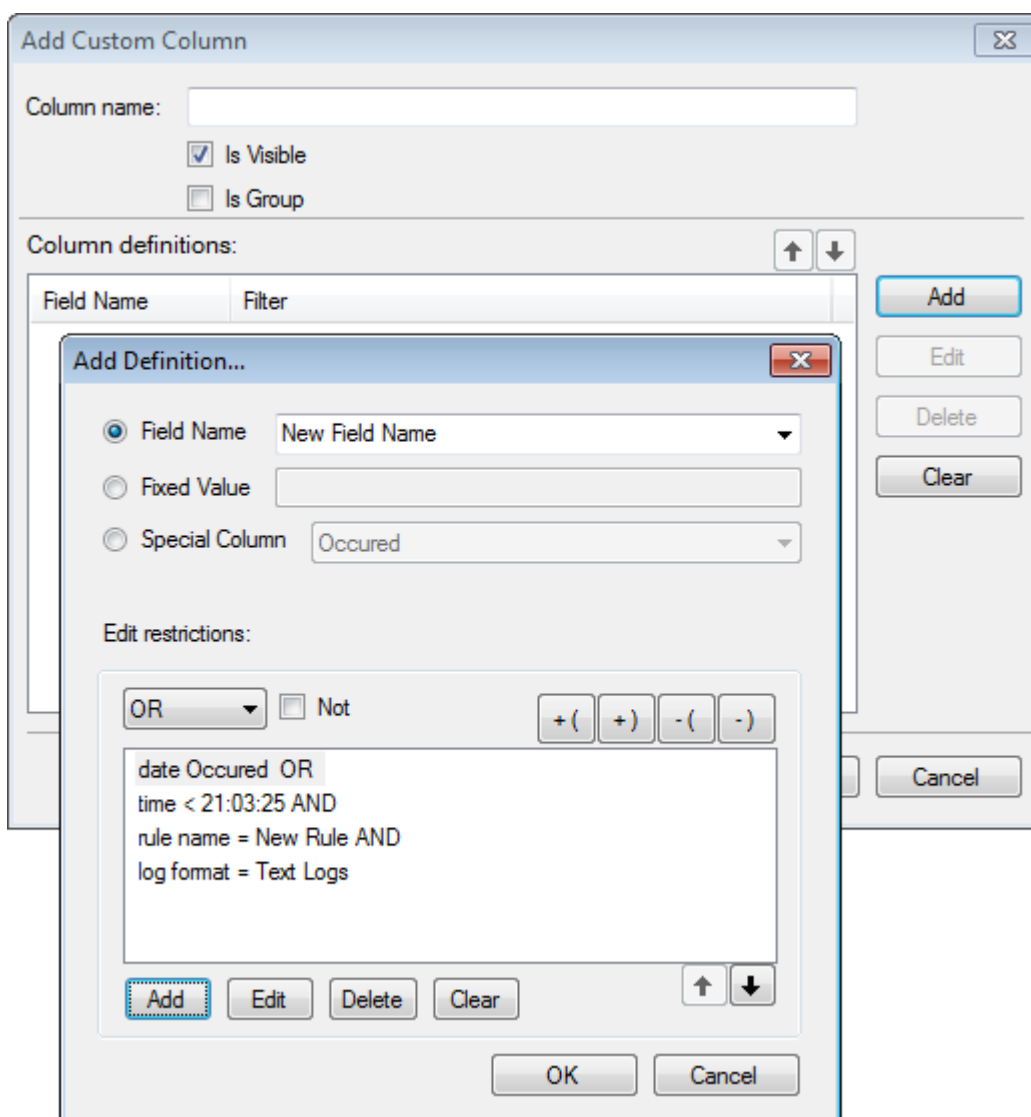
7. Click **OK** to save your settings.

5.7.2 Defining column headings

GFI EventsManager enables you to create custom columns through the **Add Custom Columns** dialog. This dialog allows you specify conditions, create a new field and add them to your report(s). Also based on conditions, this dialog enables you to further customize existing or new reports.

To add custom columns:

1. From Reporting tab ► Actions, click Create Report.
2. Click Layout tab ► **Add Existing Column**, to add default columns.
3. Click **Add Custom Column** to launch the Add Custom Columns dialog.



Screenshot 37 - Define custom column conditions

4. From the **Add Custom Column** dialog click **Add**.
5. From the **Add Definition...** dialog, configure the options described below:

Table 25 - Add Column Definition options

OPTION	DESCRIPTION
Field Name	Specify a name for the new field.
Fixed Value	Select Fixed Value if the value of the new field is going to be fixed. Specify a value as a field name. For example, to check that events always occur after 5pm, specify 5 as the fixed value instead of defining a time field and assign a value of 5.
Special Column	Special columns are predefined columns that may be used in your condition.
Edit restrictions	This section enables you to add, edit or delete field restrictions. For more information, refer to Defining Restrictions .

6. Click **OK** to save your settings.

5.8 Daily Digest

GFI EventsManager can be configured to send a summary report by email on a daily basis. The report contains a summary of the most important events collected and processed during the last 24 hours. To configure a user to receive Daily Digest emails:

1. Launch GFI EventsManager and select **Configuration** tab ► **Options**. Expand **Users and Groups** and select **Users**.
2. Right-click a user from the right pane and select **Properties**.
3. Select **General** tab and ensure that a valid email address is configured.
4. Open **Alerts** tab and select Send daily report via email.

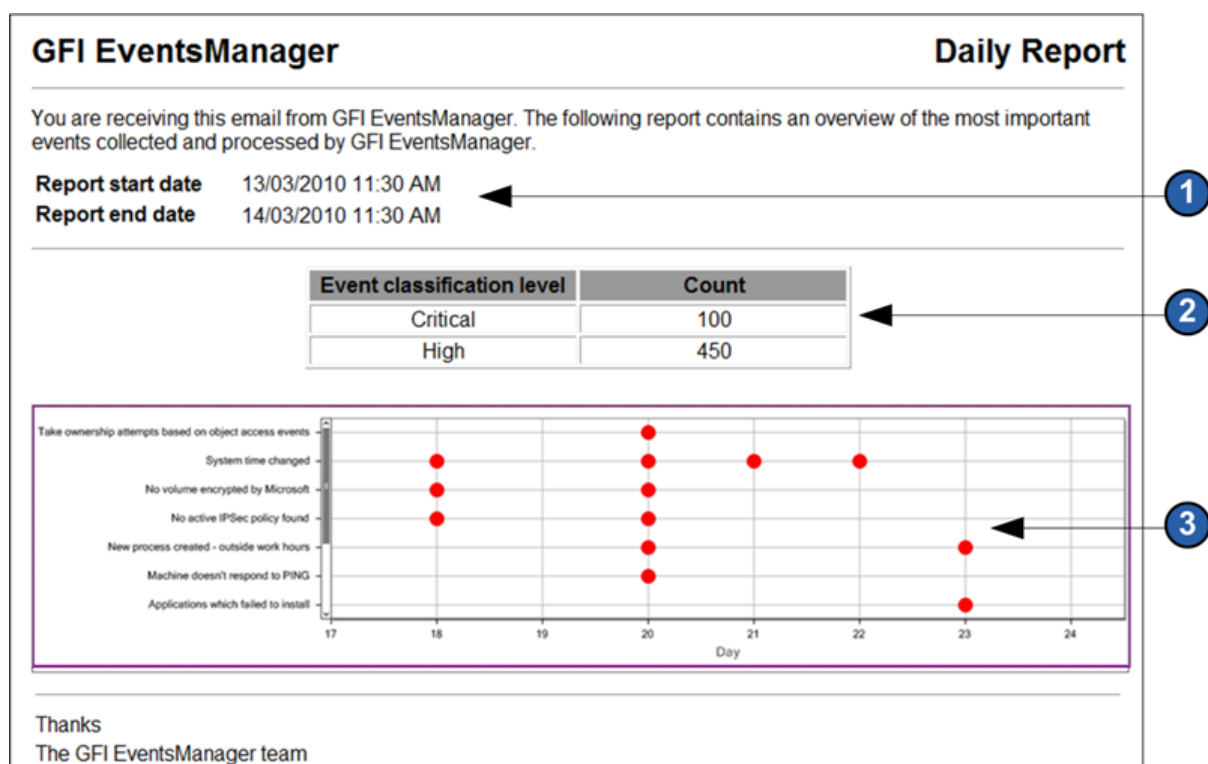
The screenshot shows the 'EventsManagerAdministrator Properties' dialog box with the 'Alerts' tab selected. The dialog has five tabs: 'General', 'Working Hours', 'Alerts', 'Member Of', and 'Privileges'. The 'Alerts' tab contains a section titled 'Specify the types of alerts this user is to receive' with a user icon. Below this, it says 'Specify the types of alerts this user should receive for events which happen during working hours or outside working hours.' There are two columns: 'During working hours' and 'Outside of working hours'. Under 'During working hours', there are three rows: 'Email alerts:' with a checked checkbox, 'Network message alerts:' with a checked checkbox, and 'SMS alerts:' with a checked checkbox. Under 'Outside of working hours', there are three rows: 'Email alerts:' with a checked checkbox, 'Network message alerts:' with a checked checkbox, and 'SMS alerts:' with a checked checkbox. At the bottom, there is a yellow highlighted section with a checked checkbox for 'Send daily report via email at', a time picker set to '12:00:00 PM', and a 'Tell me more...' link. At the very bottom are 'OK', 'Cancel', and 'Apply' buttons.

Screenshot 38 - Daily Digest email settings

5. Configure the time when the Daily Digest email is sent.
6. Click **OK**.



For more information, refer to [Configuring users and groups](#).



Screenshot 39 - Daily digest email

SECTION	DESCRIPTION
1	The start and end date of the report. The report displays the most important events collected by GFI EventsManager between the start and end date.
2	The number of Critical and High events collected in the last 24 hours.
3	This graph provides statistical information about critical events collected from all event sources in the last 24 hours.

5.9 Settings report

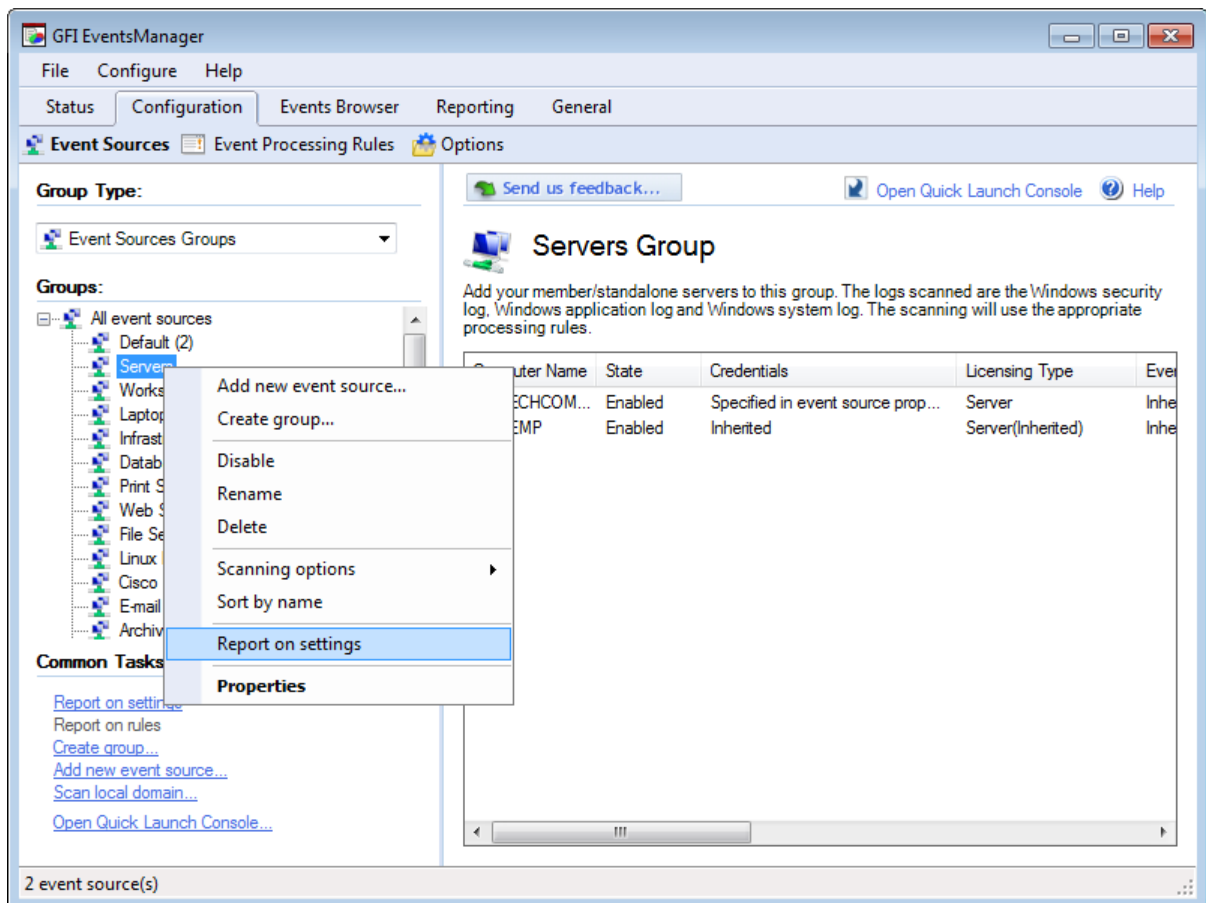
GFI EventsManager enables you to generate settings reports on event source groups. The provided information is described in the table below:

Table 26 - Settings report heading information

HEADING	DESCRIPTION
Group name	The name of the group the report is based on.
Computer name	A list of every event source in the selected group.
Scan intervals	Scanning interval for every event source in the selected group; shown in Days : Hours : Minutes : Seconds.
Rules folder	Provides a list of rule categories applied to the selected group, such as: <ul style="list-style-type: none"> » Noise reduction » Security » System health » PCI DSS requirements.
Rule sets	A granular list of rules applied on the selected group.

To generate settings report:

1. Click Configuration tab ► Event Sources.



Screenshot 40 - Generate configuration report

2. Right-click an event source group.
3. Click **Report on settings** and wait for report to generate.

GFI EventsManager™				Monitored computers
Group name	Computer name	Scan interval (D:H:M:S)	Enabled	Rule sets
Servers	TEMP	00:15:00	Yes	All rules\Windows Events\Security\Windows Filtering Platform events
				All rules\Windows Events\System Health\Disk issues
				All rules\Windows Events\System Health\Memory dumps
				All rules\Windows Events\System Health\TCP/IP issues
				All rules\Windows Events\System Health\Unexpected system shutdowns
				All rules\Windows Events\System Health\Applications crashing or hanging
				All rules\Windows Events\System Health\Windows updates
				All rules\Windows Events\System Health\Performance logs and alerts
				All rules\Windows Events\System Health\Shutdown/reboot/logoff actions
				All rules\Windows Events\System Health\Kerberos system events
				All rules\Windows Events\System Health\Kerberos Key Distribution Center system events
				All rules\Windows Events\System Health\System uptime
				All rules\Windows Events\Security Applications\Event logging system
				All rules\Windows Events\Security Applications\Windows file protection
				All rules\Windows Events\Security Applications\Windows firewall
				All rules\Windows Events\Security Applications\Windows installer
				All rules\Windows Events\Security Applications\Group Policy
				All rules\Windows Events\Security Applications\Windows services

Screenshot 41 - Settings report sample

5.10 Rules report

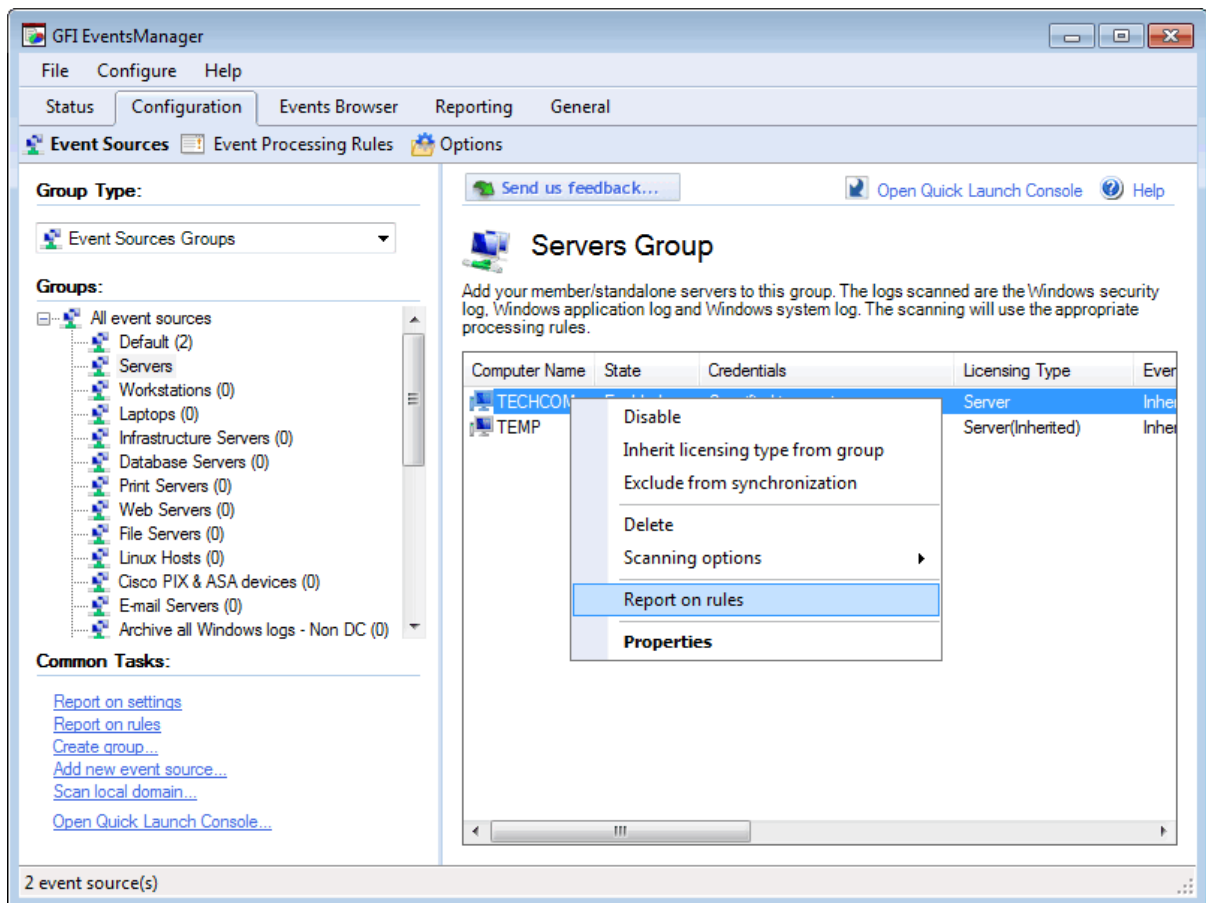
Rules reports provide a detailed view of applied rules on event sources. The rules report is described below:

Table 27 - Rules report heading information

HEADING	DESCRIPTION
Rule name	Name of the applied rule.
Importance	The classified importance level of the collect event log, such as: <ul style="list-style-type: none"> » Critical » High » Medium » Low » Noise event.
Logfile monitored	Provides the category name of the collected event log, such as: <ul style="list-style-type: none"> » Security » System Health » Application » System.
Conditions	The processing condition(s) for the selected rule. This includes: <ul style="list-style-type: none"> » Event IDs » Source » Category » User » Type » Advanced.
Actions	Describes the actions taken when the event is processed, including: <ul style="list-style-type: none"> » Archiving settings » Mail to settings » Threshold settings.

To generate rules report:

1. Click Configuration tab ► Event Sources.



Screenshot 42 - Generate configuration report

2. Right-click an event source and click **Report on rules**.

5.11 Operational history

GFI EventsManager's operational history can be exported for further analysis and archiving purposes. Operational history messages provide administrators with information as described in the table below:

Table 28 - Operational history reports

HEADING	DESCRIPTION
Date/Time	Date and time when the message was generated
Machine	Event source that generated the message
Source	Source operation that cause the message to be generated. Amongst others these include: <ul style="list-style-type: none"> » EvtCollector - message generated while collecting event logs » SNMP TrapsServer - message generated while collecting SNMP Traps Messages » EnetrpriseMaintenance - message generated during database maintenance jobs.
Job ID	An internal ID associated with the job
Log file/name	Type of logs collected. Amongst others: <ul style="list-style-type: none"> » Application » Security » Logs generated by other applications such as GFI LanGuard and GFI EndPointSecurity.
Message	The actual message generated while performing the job.

To generate Operational history reports:

1. From GFI EventsManager Management Console, click **Status ► Job Activity**.

Operational History ▼ Export data Tell me more ▲						
	Date/Time	Machine	Source	Job ID	Log format	Message
	05/12/2011 20:05:11	N/A	SNMP Traps coll...	N/A	N/A	Stopping SNMP traps server.
	05/12/2011 20:05:11	N/A	SNMP Traps coll...	N/A	N/A	Stopping SNMP traps server.
	05/12/2011 20:05:11	N/A	Syslog collector	N/A	Syslog	Stopping syslog server.
	05/12/2011 20:04:56	N/A	Syslog collector	N/A	Syslog	Starting syslog server.

Screenshot 43 - Operational history report

2. Click Export data.

Export Operation History Data

Export messages to html/csv format

Format: Html

Specify data

☒ current messages
 ☐ errors from a specific date 01 November 2011

Save files to: ogram Files\GFI\EventsManager2012\Reports\Status

You can also automate generation of these reports using esmreport.exe command line tool.

Export

Screenshot 44 - Operational history dialog

3. Specify the options described in Table 29 below and click **Export**.

Table 29 - Export operational history options

OPTION	DESCRIPTION
Format	Select the report output format. Available formats are HTML and CSV.
Current messages	Export all messages displayed in Job Activity tab.
Errors from a specific date	Specify a date and export all the messages generated on that date.
Save file to	Select checkbox to specify output location. If not selected, reports are saved in the default location within the GFI EventsManager directory.

GFI EventsManager™							Operational History for period: 2011-11-01	
Date/Time	Type	Machine	Source	Job ID	Log file/name	Message		
31/10/2011 18:41:03	Information	192.168.3.1	EvtCollector	N/A	GFI EventsManager	Start executing checks on machine 192.168.3.1..		
31/10/2011 18:41:04	Information	192.168.3.1	EvtCollector	N/A	GFI EventsManager	Executed 5 checks on machine 192.168.3.1		
31/10/2011 18:41:04	Information	192.168.3.1	EvtCollector	B3789E4A	Security	Start the collection on machine 192.168.3.1, log Security		
31/10/2011 18:41:30	Information	192.168.3.1	ProcessorService	N/A	windows	Processing 2000 windows events from machine 192.168.3.1.		
31/10/2011 18:41:33	Information	192.168.3.1	EvtCollector	1017473C	Application	Start the collection on machine 192.168.3.1, log Application		
31/10/2011 18:41:45	Information	192.168.3.1	ProcessorService	N/A	windows	Processing 2000 windows events from machine 192.168.3.1.		
31/10/2011 18:41:47	Information	192.168.3.1	EvtCollector	49851791	System	Start the collection on machine 192.168.3.1, log System		

Screenshot 45 - Operational history report sample

5.12 Activity overview

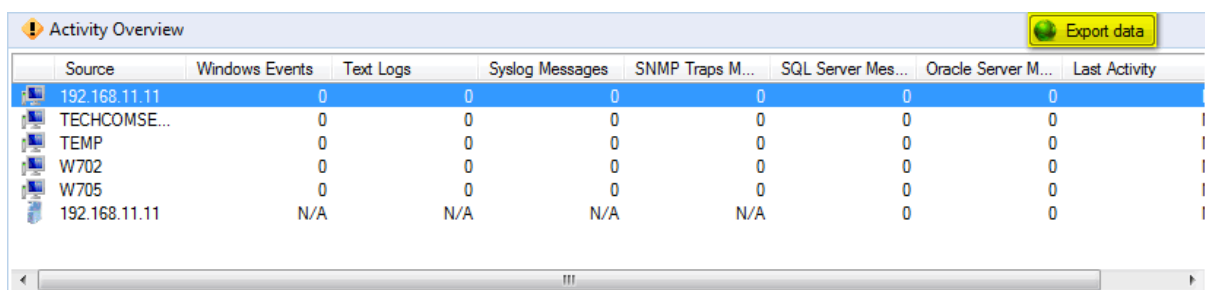
GFI EventsManager enables you to export **Activity Overview** data. Activity overview reports provide the information described in Table 30 below:

Table 30 - Activity overview headings

HEADING	DESCRIPTION
Date/Time	Date and time when the message was generated
Machine	Event source that generated the message
Source	Source operation that cause the message to be generated. Amongst others these include: <ul style="list-style-type: none"> » EvtCollector - message generated while collecting event logs » SNMP TrapsServer - message generated while collecting SNMP Traps Messages » EnetrpriseMaintenance - message generated during database maintenance jobs
Job ID	An internal ID associated with the job
Log file/name	Type of logs collected. Amongst others: <ul style="list-style-type: none"> » Application » Security » Logs generated by other applications such as GFI LanGuard and GFI EndPointSecurity
Message	The actual message generated while performing the job.

To export Activity Overview:

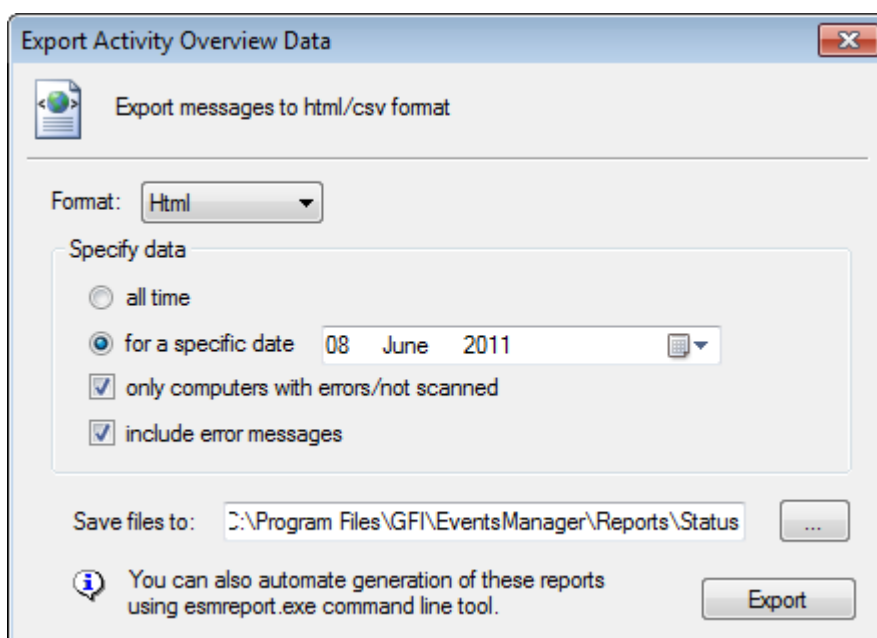
1. From GFI EventsManager Management Console, click **Status ► Statistics**.



Source	Windows Events	Text Logs	Syslog Messages	SNMP Traps M...	SQL Server Mes...	Oracle Server M...	Last Activity
192.168.11.11	0	0	0	0	0	0	
TECHCOMSE...	0	0	0	0	0	0	
TEMP	0	0	0	0	0	0	
W702	0	0	0	0	0	0	
W705	0	0	0	0	0	0	
192.168.11.11	N/A	N/A	N/A	N/A	0	0	

Screenshot 46 - Activity overview : Export button

2. Click Export data.



Export Activity Overview Data

Export messages to html/csv format

Format: **Html**

Specify data

☐ all time

☒ for a specific date **08 June 2011**

☒ only computers with errors/not scanned

☒ include error messages

Save files to: **C:\Program Files\GFI\EventsManager\Reports\Status**

You can also automate generation of these reports using esmreport.exe command line tool.

Export

Screenshot 47 - Activity overview dialog

3. Configure the options described in and click **Export**.

Table 31 - Export operational history options

OPTION	DESCRIPTION
Format	The report output format. Available formats are HTML and CSV.
All time	Export all messages displayed Activity Overview .
From a specific date	Specify a date to export all messages generated on that date.
Only computers with errors/	Export only data of computers with scanning issues.
Include error messages	Select this option to include the generated error message.
Save files to	Displays the default export location.

GFI EventsManager™		Activity Overview for period: 2011-11-01					
Source	Windows Events	W3C Events	Syslog Messages	SNMP Traps Messages	SQL Server Messages	Oracle Server Messages	Last Activity
285075	0	0	0	0	0	0	01/11/2011 19:21:04
17705	0	0	0	0	0	0	01/11/2011 19:22:14
8050	0	0	0	0	0	0	01/11/2011 19:21:10
12961	0	0	0	0	0	0	01/11/2011 19:21:04

Screenshot 48 - Activity overview report sample

6.1 Introduction

Event sources are networked computers and devices that are accessed and processed by GFI EventsManager. The **Events Sources** sub-tab (**Configuration ► Event Sources**), enables you to organize these event sources into specific groups. You can create new groups or use the default ones to distinctively configure and organize your event sources. The following sections contain information about managing event sources:

- » [Managing event sources groups](#)
- » [Adding event sources](#)
- » [Configuring event source properties](#)
- » [Microsoft SQL Server sources](#)
- » [Oracle Server sources](#)
- » [GFI LanGuard event sources](#)
- » [GFI EndPointSecurity event sources](#)

6.2 Managing event sources groups

Grouping event sources into Event Source Groups improves the speed at which you configure event sources. Once an event source group is configured, every member of that particular group inherits the same settings.

To create a new event source group:

1. Click Configuration tab ► Event Sources.
2. From Group Type select Event Sources Groups.
3. Right-click All event sources and select Create group...
4. Select the license type. Choose between **Workstation** and **Server** license.

New Event Sources Group

Windows Event Log | W3C Logs | Syslog | SNMP Traps | Audit

General | Logon Credentials | Licensing type | Operational Time

Enter a group name and description for the computers you want to include in this group.

Group Name :
NewGroupName

Description:
New group description.

☒ Enable collection of logs from this computer group

Schedule scanning

☒ Real-Time i.e. once every 5 seconds

☐ Once every: 15 Minutes

Next scan: 22/10/2011 01:38:45

OK Cancel Apply

Screenshot 49 - Add new event source group

5. Key in a valid name and a description (optional). Select the tabs described below, and configure the available options:

Table 32 - Event source group options

TAB NAME	DESCRIPTION
General	Enable collection of events and schedule the scanning process. For more information, refer to Configuring general event source properties .
Logon credentials	Configure the username and password used to login target machines and collect information. For more information, refer to Configure Logon Credentials .
Licensing type	Select the type of license to use. Select between workstation and server license.
Operational time	Configure the operational time that computers are normally used. For more information, refer to Configure operational time .
Audit	Enable GFI EventsManager auditing on target computers and configure the audit to perform. For more information, refer to Configure GFI EventsManager Auditing .
Windows Event Log	Specify the logs to collect and configure archive settings for Windows event logs. For more information, refer to Collecting Windows events .
W3C Logs	Specify the logs to collect and configure archive settings for W3C logs. This tab is only available when creating a server group. For more information, refer to Collecting W3C logs .
Syslog	Specify the logs to collect and configure archive settings for Syslogs. This tab is only available when creating a server group. For more information, refer to Collecting Syslogs .
SNMP Traps	Specify the logs to collect and configure archive settings for SNMP Traps. This tab is only available when creating a server group. For more information, refer to Collecting SNMP Traps .

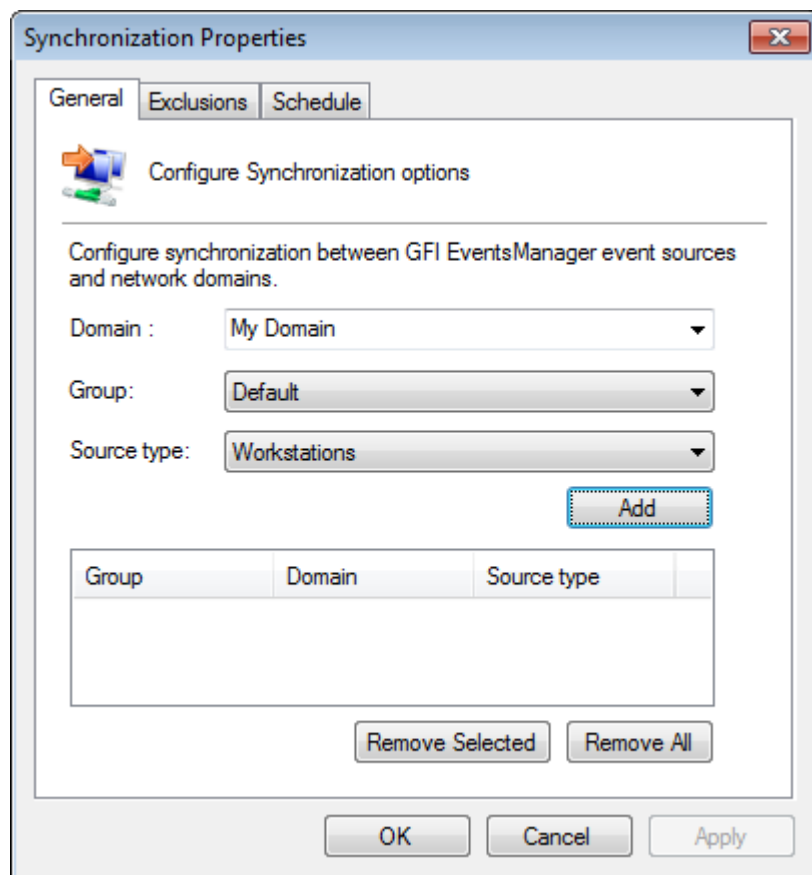
5. Click **OK** to save changes.

6.2.1 Edit synchronization options

GFI EventsManager enables you to synchronize domains with event sources groups. When the synchronization is configured, every new domain member is added automatically to GFI EventsManager event sources.

To edit synchronization options:

1. From Configuration tab ► Group Type, select Event Sources Groups.
2. Select All event sources node. From Actions, click Edit synchronization options.



Screenshot 50 - Synchronization properties - General tab

3. Select **General** tab and configure the options described below:

Table 33 - Synchronization properties - General tab

OPTION	DESCRIPTION
Domain	Select the domain name from the list or key in a valid domain name.
Group	Select the GFI EventsManager group name where to add the discovered event sources.
Source type	Select the type of computers discovered in the selected domain that will be added to the selected GFI EventsManager group.

4. To include the synchronization click **Add**.

5. Repeat steps 3 to 4 for each synchronization. The table below shows some examples of possible synchronizations that can be configured:

Table 34 - Example of synchronizations

GROUP	SYNC WITH
Archive all Windows logs-Non DC	Generic Servers
Workstations	Workstations
E-mail Servers	Exchange Servers
Archive all Windows logs - DC	Domain Controllers

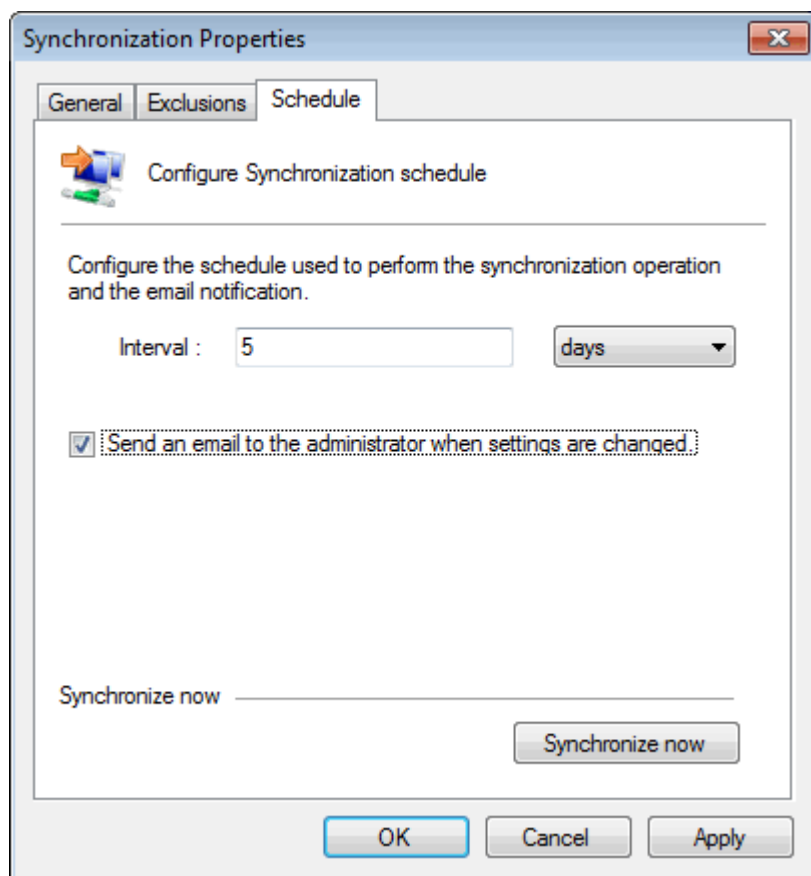
GROUP	SYNC WITH
Servers	ISA Servers

6. (Optional) Select **Exclusions** tab to configure the list of computers that will be excluded from the synchronization. Click **Add** and key in a computer name to exclude.



Event sources that are already part of an event source group will be automatically excluded from synchronization. For more information, refer to [Manage event sources](#).

7. Select **Schedule** tab to configure when the synchronization should be performed.



Screenshot 51 - Synchronization properties -Schedule tab

8. Key in a valid interval in hours or days.

9. (Optional) Select **Send an email to the...** to send an email notification when event sources are changed after synchronization.

10. (Optional) Click **Synchronize now** to synchronize event sources immediately.

11. Click **OK**.

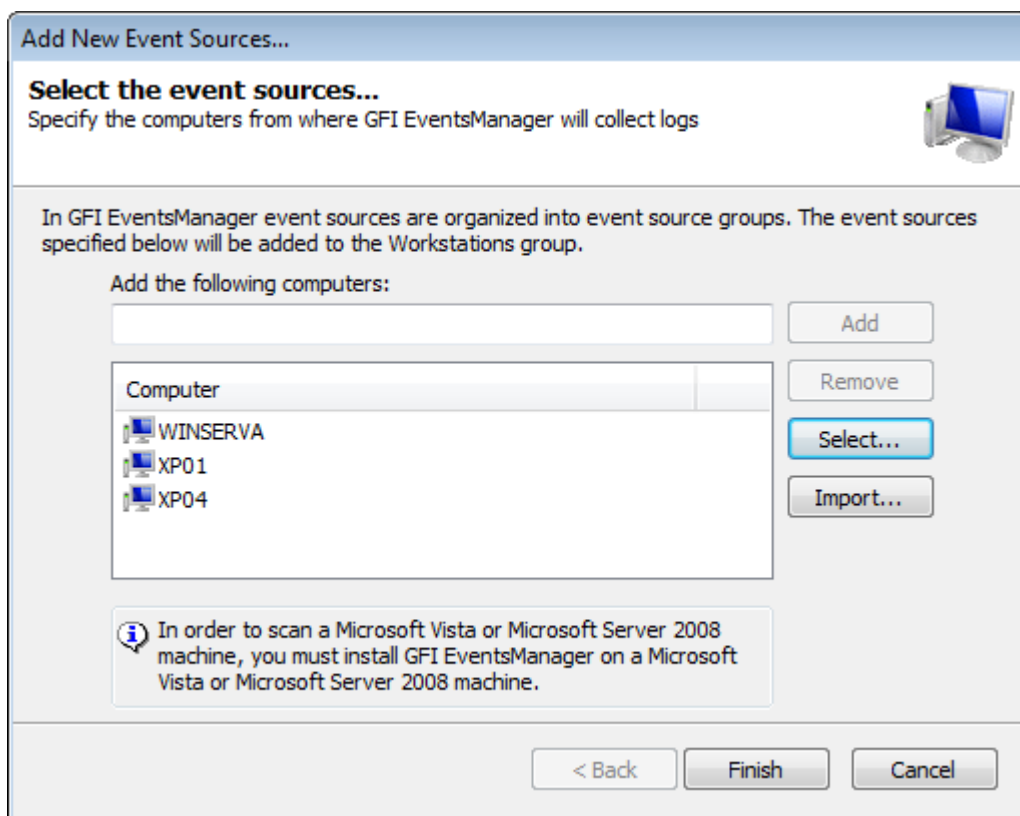


Adding Event Sources manually to a synchronized group is not allowed in GFI EventsManager.

6.3 Adding event sources

To add a new event sources to a computer group:

1. Click Configuration tab ► Event Sources.
2. From Group Type, select Event Sources Groups.
3. Right-click a computer group of your choice and select **Add new event source...**



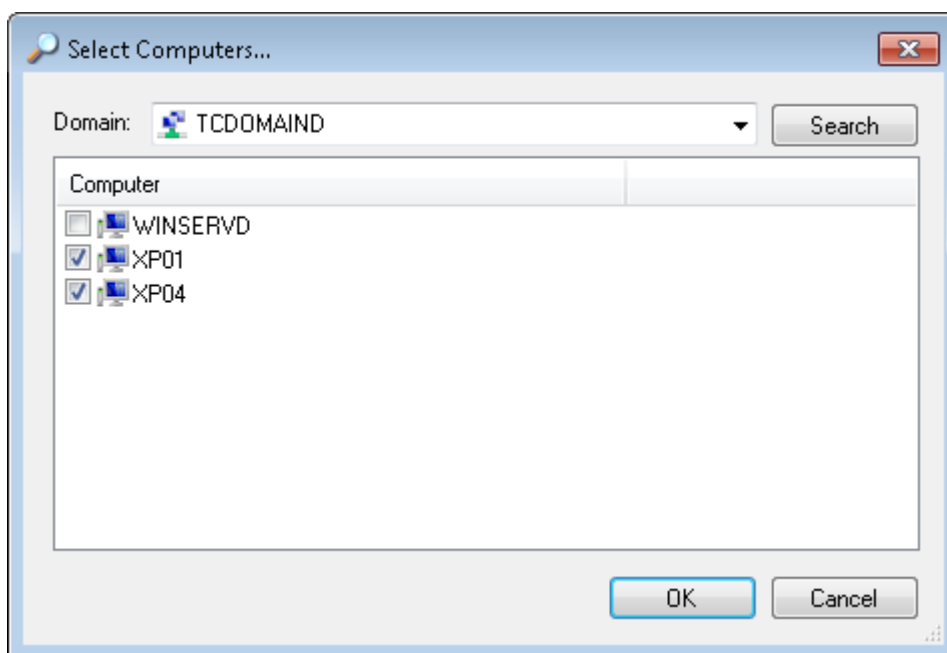
Screenshot 52 - Add new event source wizard

4. Specify the name or IP of the new event source and click **Add**. Repeat until you have specified all the event sources to add to this group.



Since Syslog and SNMP traps use the IP address to determine the source of an event, it is recommended to use the source IP instead of the domain name when retrieving Syslog and SNMP traps from target machines.

5. (Optional) Click **Select** to browse the network for existing domains and computers. Select the domain from the **Domain** drop down list and select the computers to add.



Screenshot 53 - Browse the network for connected computers

6. (Optional) Click **Import...** to import computers from a text file. Ensure that the text file contains only one computer name or IP per line.

7. Click **Finish** to finalize your settings. GFI EventsManager will attempt to collect logs from the configured sources immediately.



If synchronization is not enabled, you can use the **Network Discovery Wizard** to automatically search and add event sources. To launch **Network Discovery Wizard**, right-click **All event** sources from the event sources tree and select **Scan local domain**. For more information, refer to [Processing events from the local domain](#).

6.4 Configuring event source properties

GFI EventsManager allows you to customize the event source parameters to suit the operational requirements of your infrastructure. You can configure these parameters on a:

- » Computer by computer basis
- » Group by group basis.

To configure event source properties:

1. From Configuration tab ► Group Type, select Event Sources Groups.

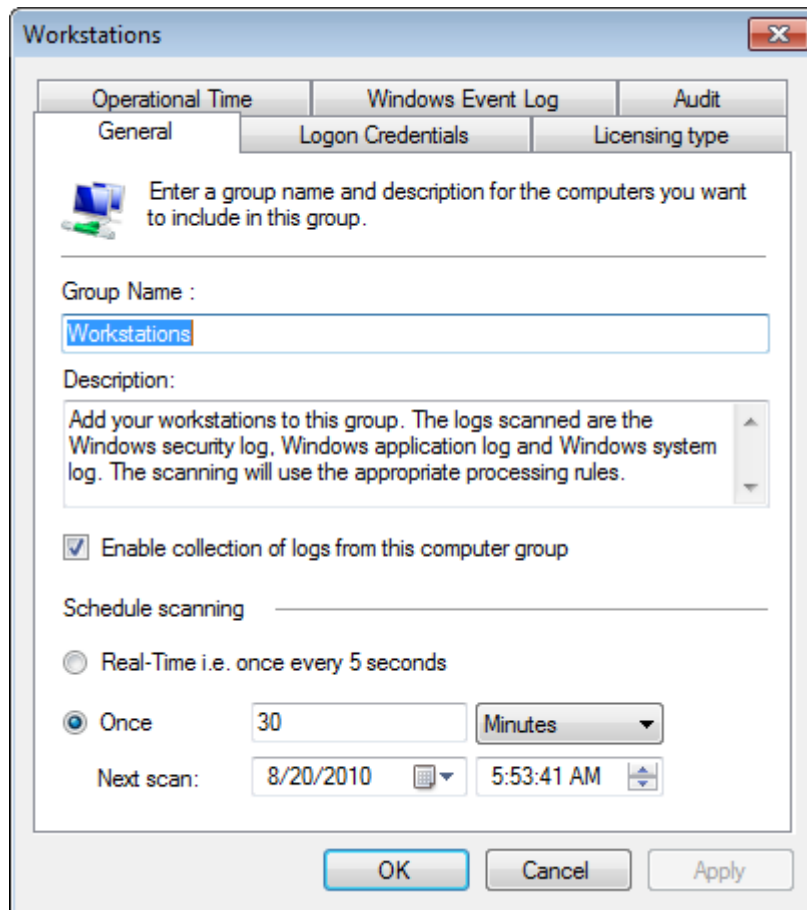
3. To configure the parameters of:

PARAMETER	DESCRIPTION
Computer group	Right-click on the computer group to be configured and select Properties .
Particular computer in a group	Right-click on the required computer and select Properties .

4. Click required tabs and configure the respective parameters accordingly. More information on how to configure these parameters is provided in the following sections:

- » [Configuring general event source properties](#)
- » [Configuring logon credentials](#)
- » [Configuring operational time](#)
- » [Configuring event source auditing](#)
- » [Configuring event processing parameters](#)

6.4.1 Configuring general event source properties



Screenshot 54 - Event sources properties dialog

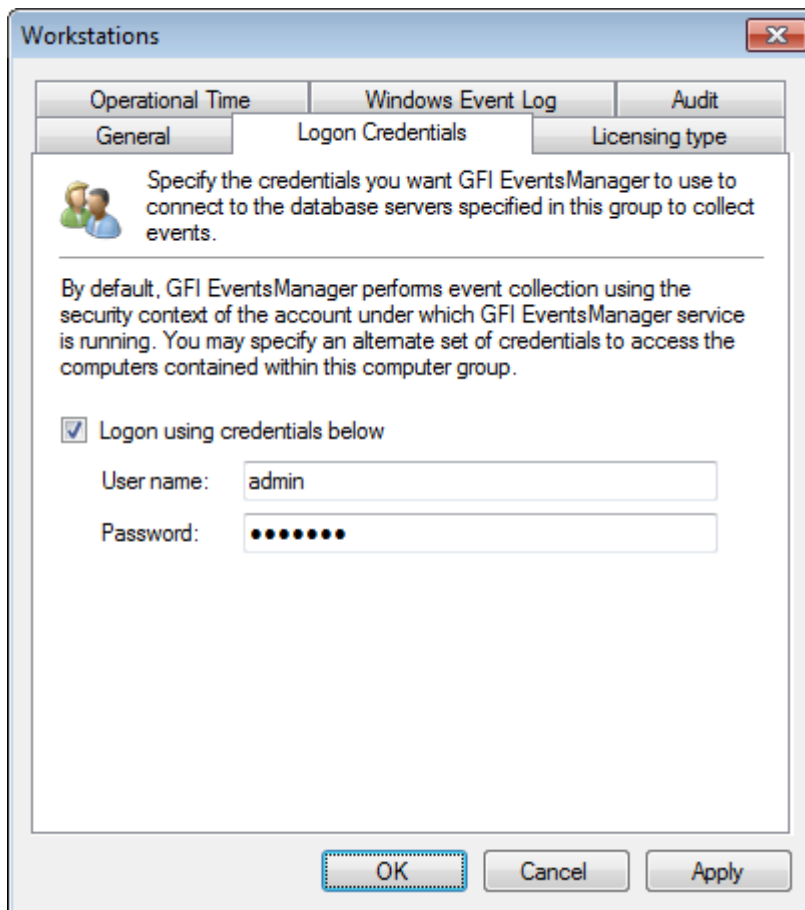
Use the General tab in the properties dialog to:

- » Change the name of a computer group
- » Enable/disable log collection and processing for the computers in a group
- » Configure log collection and processing frequency.

6.4.2 Configuring Logon Credentials

During event processing, GFI EventsManager must remotely log-on to the target computers. This is required in order to collect log data that is currently stored on the target computers and to pass this data on to the event processing engine(s).

To collect and process logs, GFI EventsManager must have administrative privileges over the target computers. By default, GFI EventsManager will log-on to target computers using the credentials of the account under which it is currently running; however, certain network environments are configured to use different credentials to log on to workstations and servers with administrative privileges. As an example for security purposes, network administrators can setup a dedicated account that has administrative privileges over workstations only and a different account that has administrative privileges over servers only.



Screenshot 55 - Configuring alternative logon credentials

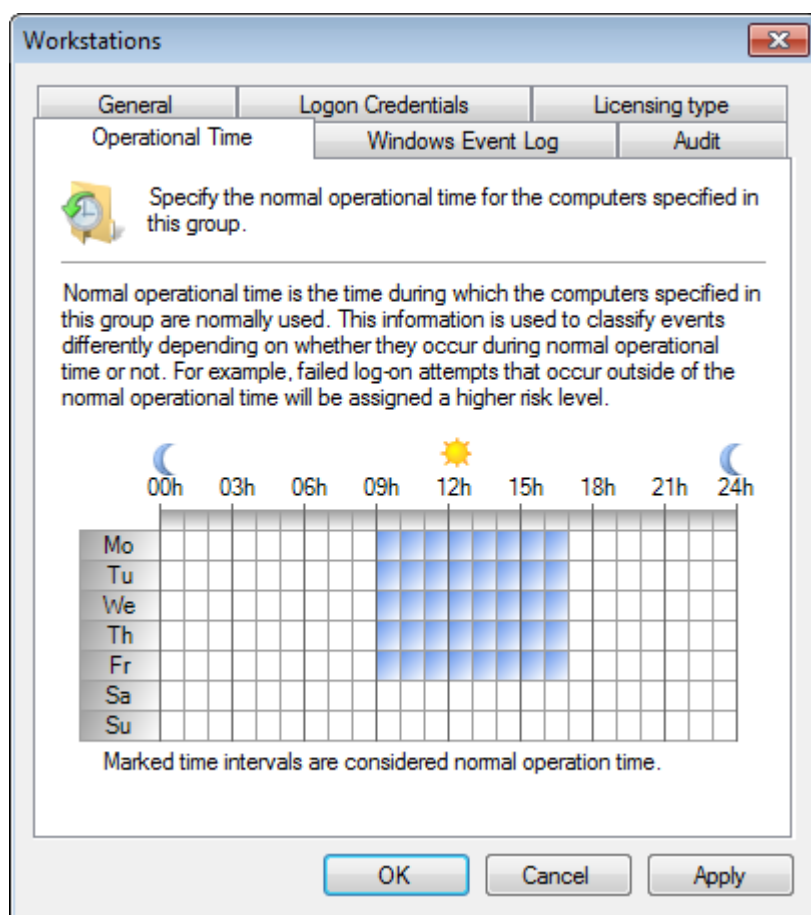
GFI EventsManager, allows you to configure a dedicated set of logon credentials for individual event sources and groups. To configure a set of credentials for a particular computer group:

1. Right click on an event source and click on **Properties**
2. Click **Logon Credentials** tab
3. Specify the login name and password and click **OK**.

6.4.3 Configuring operational time

GFI EventsManager includes an **Operational Time** option through which you specify the normal working hours of your event sources. This is required so that GFI EventsManager can keep track of the events that occur both during and outside working hours.

Use the operational time information for forensic analysis; to identify unauthorized user access, illicit transactions carried outside normal working hours and other potential security breaches that might be taking place on your network.



Screenshot 56 - Specify operational time

Operational time is configurable on computer group basis. This is achieved by marking the normal working hours on a graphical operational time scale which is divided into one hour segments.

6.4.4 Configure event source auditing

GFI EventsManager collects additional data from the network using a checking engine. If auditing is enabled on an event source, the audit will be executed before collecting events and creates relative Windows events.

For example, when executing **Check slow connection**, the script performs a PING request and records the response time. If the response time is more than 500 milliseconds, the script creates a Windows event in the Application log of the target machine.



If an audit fails to execute due to network disconnection or insufficient permissions, no windows events are created.

Table 35 - Event sources: Audit policy options

CHECK LIST	DESCRIPTIONS
Check audit policy	Checks the status of audit policies on target machines. If an audit policy is disabled, a Windows event is created. For more information on how to enable audit policies, refer to Step 2: Enable additional auditing features section in this manual.
Check disk space	Checks the target machine disk drives' free space. If a disk has less than 10% free space, a Windows event is created. Amongst others, the Windows event contains information on disk drive name and storage space.
Check inactive domain machines	Checks the domain for inactive machines. A machine can be inactive if no log in requests were sent during the previous 30 days. If inactive machines are found, a Windows event is created.
Check inactive users	Checks domain for inactive user accounts. A user account is inactive if no log in requests were sent during the previous 30 days. If inactive accounts are found, a Windows event is created.

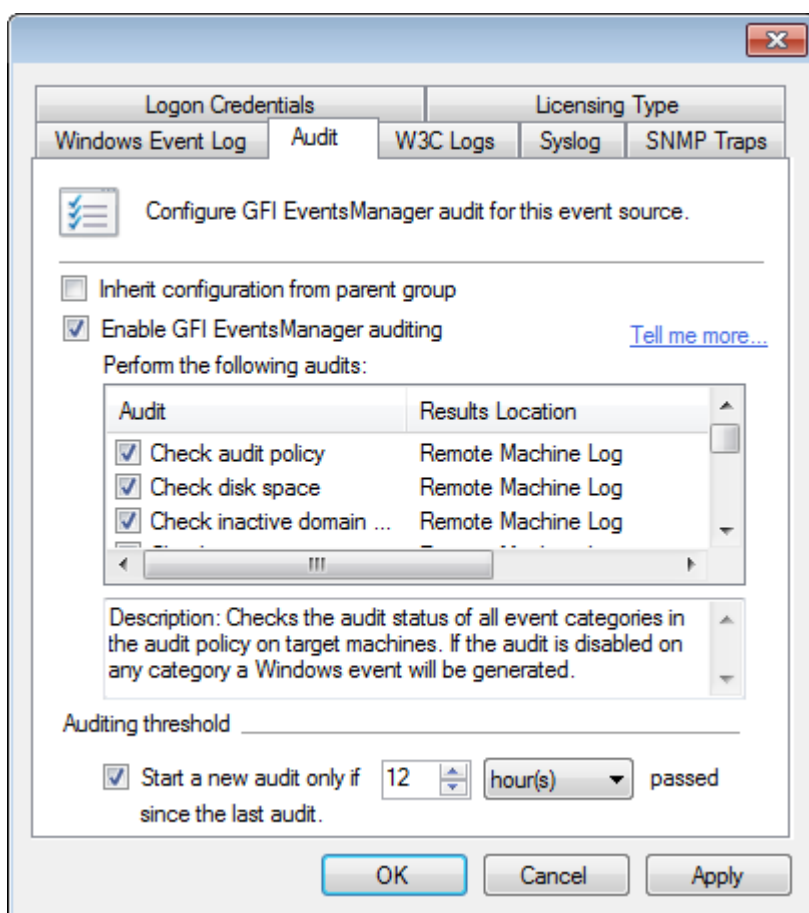
CHECK LIST	DESCRIPTIONS
Check IPSec policies status	Checks status of IPSec policies on target machines, if any. If IPSec policies exist and are inactive, a Windows event is created.
Check Microsoft firewall status	Checks status of any Microsoft Windows Firewall or ISA servers on target machines. If a Firewall exists and is off, a Windows event is created.
Check slow connection	The script performs a PING request and records the response time. If the response time is more than 500 milliseconds, the script creates a Windows event.
Check volumes encrypted by Microsoft	Checks if there are volumes encrypted using Microsoft products (e.g. Bit Locker), on target machines. If volume encryption is not used, a Windows event is created.



To configure GFI EventsManager auditing event processing rules, navigate to **Configuration tab ► Event Processing Rules** and from the **Rule Folders** tree, select **Windows Events**. For more information, refer to [Using event processing rules](#).

To enable and configure GFI EventsManager auditing:

1. Right-click an event source or an event source group, and click **Properties**.



Screenshot 57 - Event source properties: Audit tab

2. From the **Properties** dialog, select **Audit** tab and configure the options described below:

Table 36 - Auditing options

OPTION	DESCRIPTION
Inherit configuration from parent group	Select this option to use the settings configured in the parent group.
Enable GFI EventsManager auditing	Select this option to enable GFI EventsManager auditing.
Perform the following audits	Select the audits to perform on target machines.

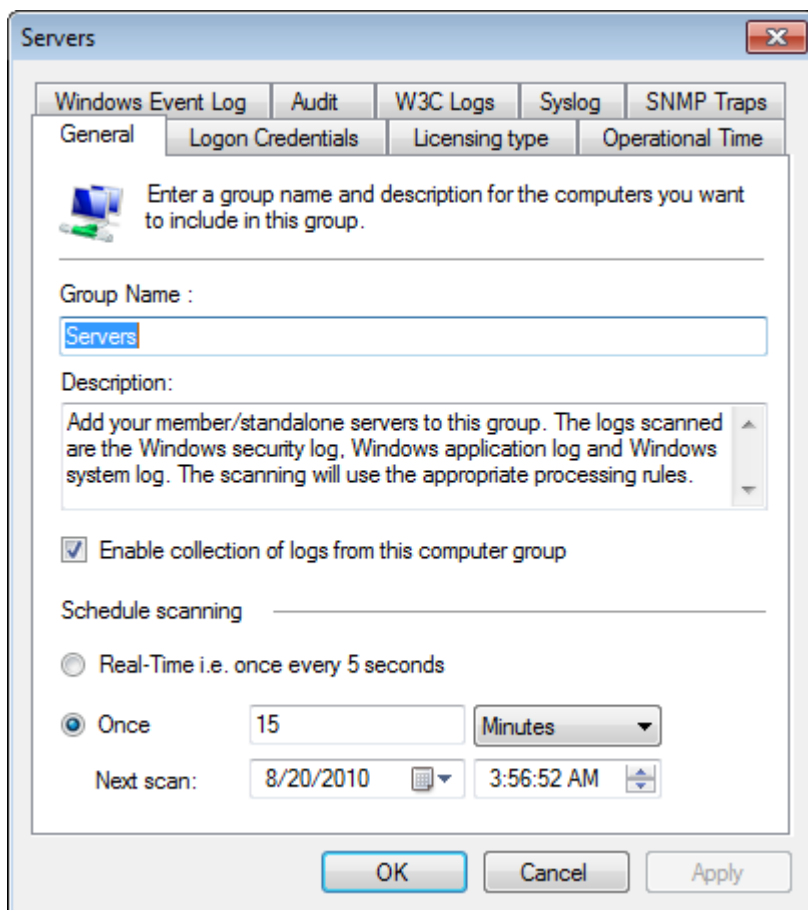
OPTION	DESCRIPTION
Start a new audit only if...	Select this option and configure the threshold time between audits. GFI EventsManager will wait for the defined interval before starting a new audit check.

Audit checks are executed before scanning windows events, if the audit check is successful a windows log event is created on the target machine. This may create a large number of events and it is recommended to configure and use the **Auditing threshold**. When using the **Auditing threshold** GFI EventsManager will wait for a pre-defined interval before starting a new audit check.

4. Click **OK** to save changes.

6.4.5 Configuring event processing parameters

To configure event processing parameters:



Screenshot 58 - Event-processing configuration tabs

1. Click Configuration tab ► Group Type ► Event Sources Groups.
2. From the **Groups** list, right-click the group to configure and select **Properties**.
3. Use the **Windows Event Log** tab, **W3C Logs** tab, **Syslog** tab and **SNMP Traps** to configure the required event processing parameters.



For more information, refer to [Using event processing rules](#).

6.5 Microsoft SQL Server sources

6.5.1 Creating a new Microsoft SQL Server Group

To add a Microsoft SQL Server group:

1. Click Configuration tab ► Event Sources. From Group Type, select Database Servers Groups.



Screenshot 59 - Database Servers Groups

2. From Groups, right-click Microsoft SQL Servers and select Create group.
3. Select **Microsoft SQL Server** as the server type and from the **General** tab configure the options described in the table below:

Table 37 - Microsoft SQL Database group: General tab

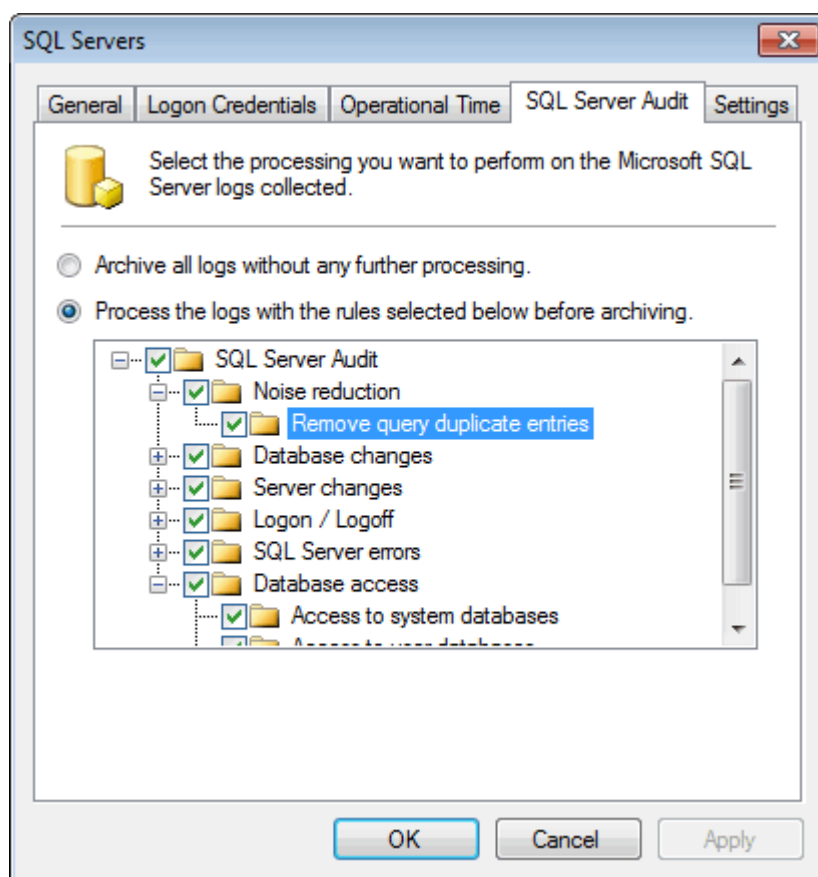
OPTION	DESCRIPTION
Group Name	Key in a group name to identify the Microsoft SQL server group.
Description	(Optional) Key in a description.
Collects logs from the database servers included in this group.	Enable option to collect database events from all servers in this group.

4. Select **Logon Credentials** tab and configure the options described below:

Table 38 - Microsoft SQL Database group: Logon Credentials

OPTION	DESCRIPTION
Use Windows authentication	Connect to the Microsoft SQL Database using windows authentication.
Use SQL Server authentication	Connect to Microsoft SQL Database using a Microsoft SQL Database user account. Key in a username and password.

5. Select **Operational Time** and configure the operational time when the database is normally used.



Screenshot 60 - Microsoft SQL Database group - SQL Server Audit tab

6. Select **SQL Server Audit** tab and configure the options described below:

Table 39 - Microsoft SQL Database group -SQL Server Audit

OPTION	DESCRIPTION
Archive all logs without further processing	Archive events in GFI EventsManager database backend without processing.
Process the logs with the rules selected below before archiving	Specify the rules to perform before archiving events in GFI EventsManager database backend.
Archive all scanned events in folder storage.	Archives collected events into GFI EventsManager storage folder. For more information, refer to Configure storage folder .

7. Select **Settings** tab and configure the options described in below:

Table 40 - Microsoft SQL Database group - Settings

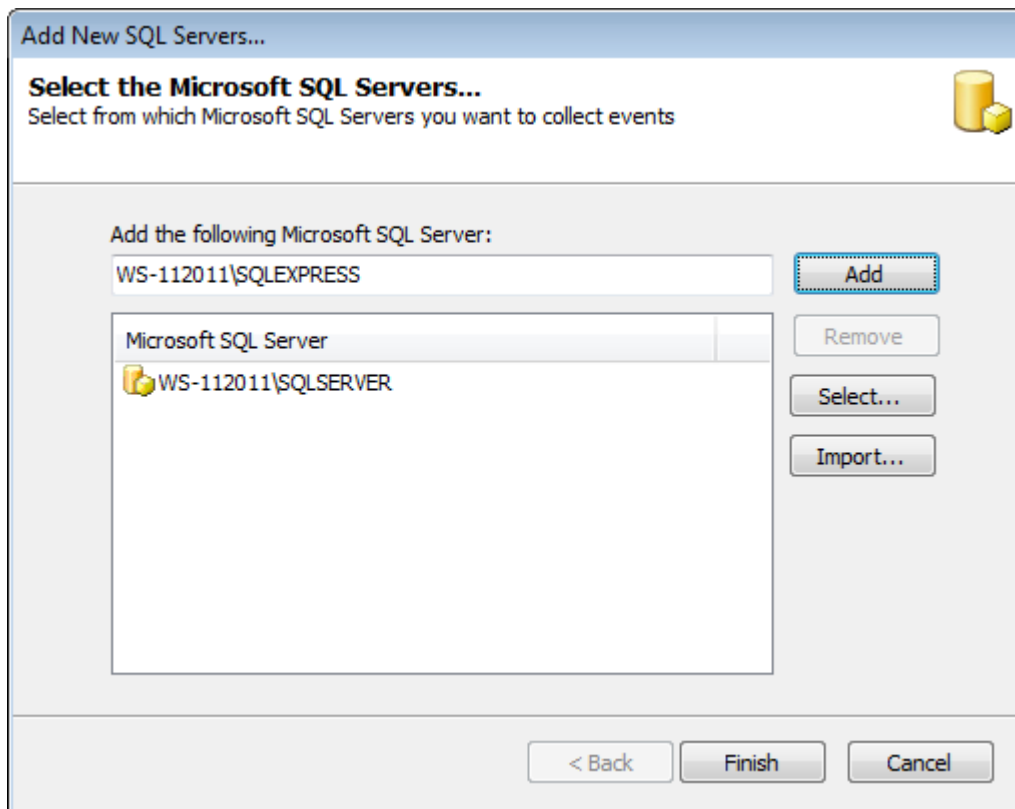
OPTION	DESCRIPTION
Scan all the events for all databases	All Microsoft SQL Server events are collected and processed by GFI EventsManager.
Scan only security events for all databases	Only security events are collected and processed by GFI EventsManager.

8. Click **OK**

6.5.2 Adding a new Microsoft SQL Server event source

To add a new Microsoft SQL Server source:

1. Right-click the database group and select **Add new SQL Server**.



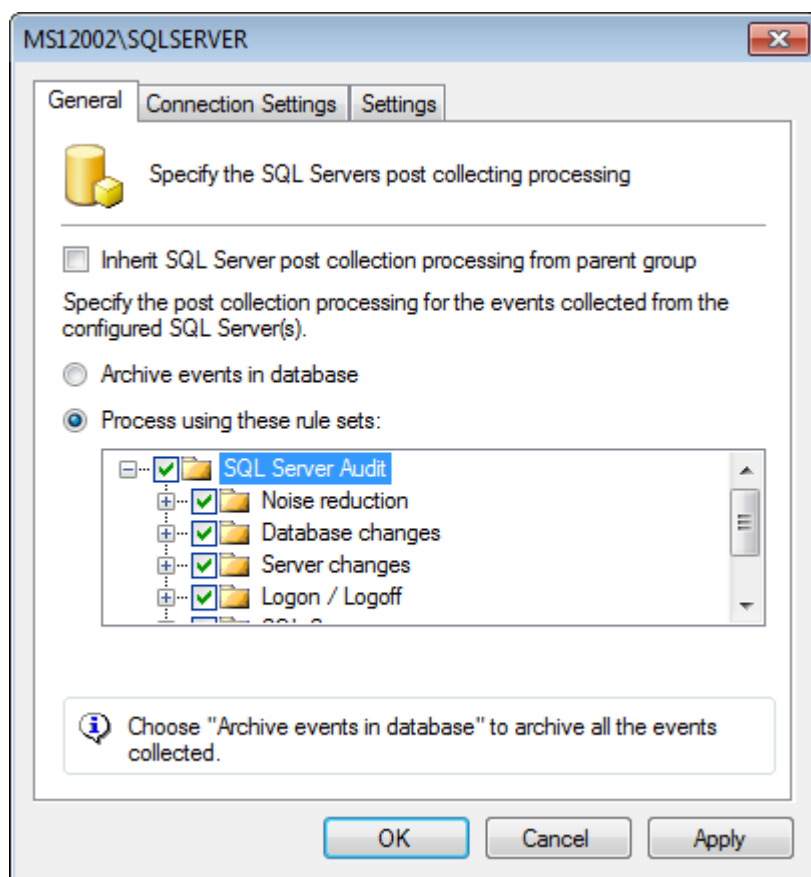
Screenshot 61 - Add new Microsoft SQL server

2. Key in the server name or IP and click **Add**.



Use **Select** and **Import** to search the network for SQL Servers or import list of SQL servers from a text file respectively. Click **Finish** when ready.

3. From Groups, select Microsoft SQL Servers. From the right pane, double-click the Microsoft SQL Database instance.

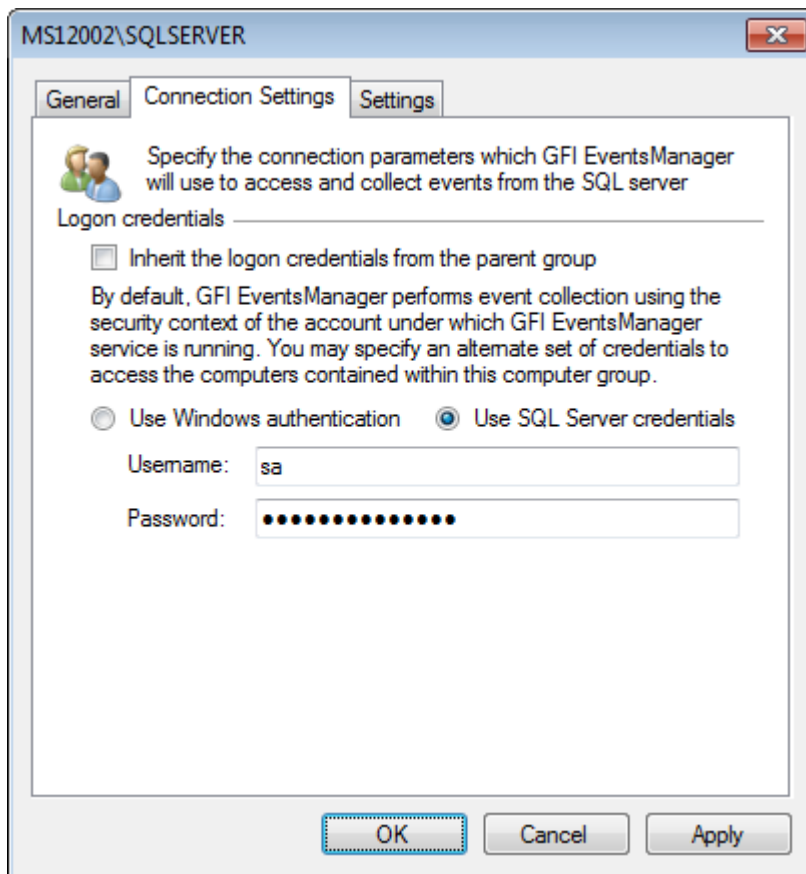


Screenshot 62 - Microsoft SQL Database properties: General tab

4. In the General tab, configure the options described below:

Table 41 - Microsoft SQL Database - General tab options

OPTION	DESCRIPTION
Inherit SQL Server post collecting processing from parent group.	Inherits all settings from the parent group.
Archive events in database	Archive all events in GFI EventsManager database backend without processing.
Process using these rule sets	Archive all events using the specified rules. Select the rules to apply.

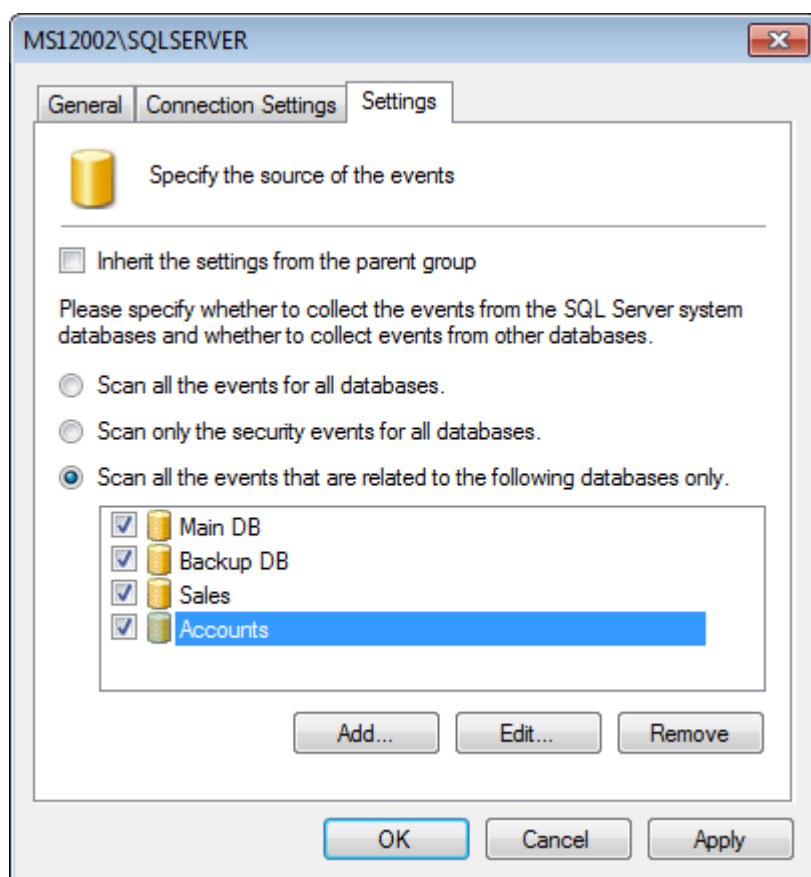


Screenshot 63 - Microsoft SQL Database properties: Connection Settings tab

5. Select **Connection Settings** and configure the options described below:

Table 42 - Microsoft SQL Database - Connection Settings tab

OPTION	DESCRIPTION
Inherit the logon credentials from the parent group	Select this option to inherit login settings from the parent group.
Use Windows authentication	Connect to Microsoft SQL Database using windows authentication.
Use SQL Server credentials	Connect to Microsoft SQL Database using a Microsoft SQL Database user account. Key in a username and password.



Screenshot 64 - Microsoft SQL Database properties: Settings tab

6. Select **Settings** tab and configure the options described below:

Table 43 - Microsoft SQL Database - Settings tab options

OPTION	DESCRIPTION
Inherit the settings from the parent group	Inherits settings from the parent group.
Scan all the events for all databases	Scan all databases and collect all events from the Microsoft SQL Server.
Scan only the security events for all databases	Scan all databases and collect only security events from the Microsoft SQL Server.
Scan all the events that are related to the following databases only.	Collect all events from the selected databases. Use Add , Edit and Remove to manage database sources.

7. Click **OK**.

6.6 Oracle Server sources

GFI EventsManager enables you to collect and process events generated by Oracle Relational database management systems. The following audits are collected and processed by GFI EventsManager:

Table 44 - Oracle Server supported audits

AUDIT	DESCRIPTION
Session auditing	Audit user sessions and database access.
Statements auditing	Audit SQL statements.
Object auditing	Audit queries and statements related to specific objects.

The following Oracle Database versions are supported:

- » Oracle Database 9i
- » Oracle Database 10g
- » Oracle Database 11g

6.6.1 Pre-configuration settings for Oracle servers

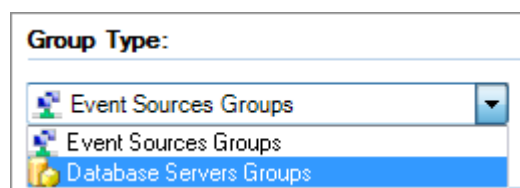
Table 45 - Oracle Server configuration stages

PRE-CONFIGURATION STEP	DESCRIPTION
Step 1	Before collecting events from Oracle servers ensure that the account used to connect, set audits and access the audit table has the necessary permissions.
Step 2	<p>Enable auditing on the Oracle server by changing startup parameters. To enable auditing:</p> <ol style="list-style-type: none">1. Startup parameters for the Oracle servers are stored in <Oracle Home Directory>\admin\<Oracle SID>\pfile\init.ora.2. Locate and open the parameters file using a text editor.3. Locate AUDIT_TRAIL parameter and change the default value to 'db' or 'db_extended' ('db,extended' on latest versions of Oracle).4. Save and restart the Oracle server.

6.6.2 Adding a new Oracle Server group

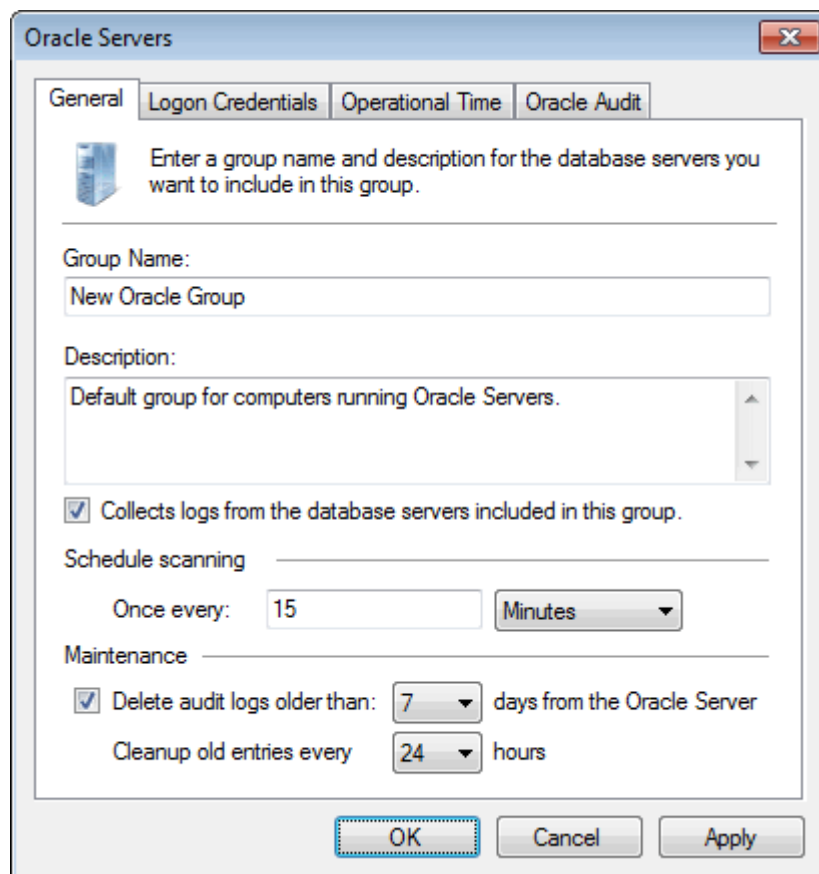
To add a new Oracle Database group:

1. Click Configuration ► Event Sources and from the Group Type, select Database Servers Groups.



Screenshot 65 - Database Servers Groups

2. From the right panel, right-click **Oracle Servers** and select **Create group...**



Screenshot 66 - Oracle Database group - General tab

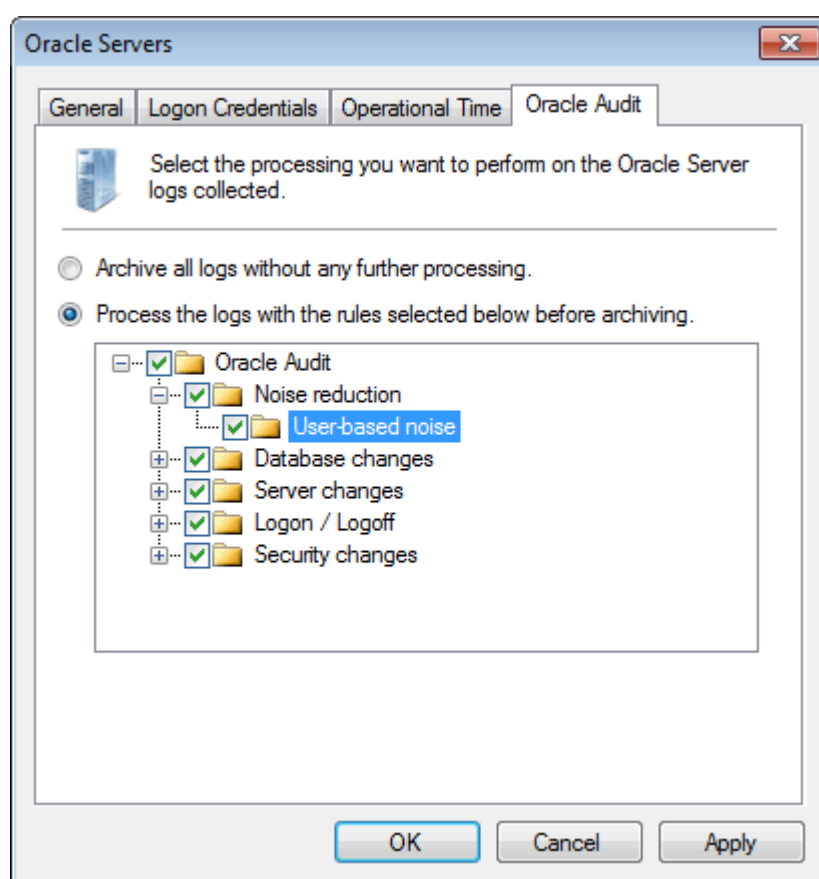
3. In the General tab, configure the options described in below:

Table 46 - Oracle Database group - General tab

OPTION	DESCRIPTION
Group Name	Key in a group name to identify the Oracle Database group.
Description	Optional, key in a description.
Collects logs from the database servers included in this group	Collects events from the event sources in the Oracle group. Once this option is enabled, configure the Schedule scanning and Maintenance options.
Schedule scanning	Specify the frequency to collect events on a pre-defined schedule.
Maintenance	Oracle audit events are stored in a specific audit table on the Oracle server. To prevent excessive audit table growth, configure the options in this section to delete audit logs and old entries on a pre-defined time.

4. Select **Logon Credentials** tab and key in a valid username and password to connect to the Oracle server.

5. Select **Operational Time** tab and configure the normal operational time of the Oracle Database servers in this group.



Screenshot 67 - Oracle Database group - Oracle Audit tab

6. Select **Oracle Audit** and configure the options described below:

Table 47 - Oracle Database group - Oracle Audit

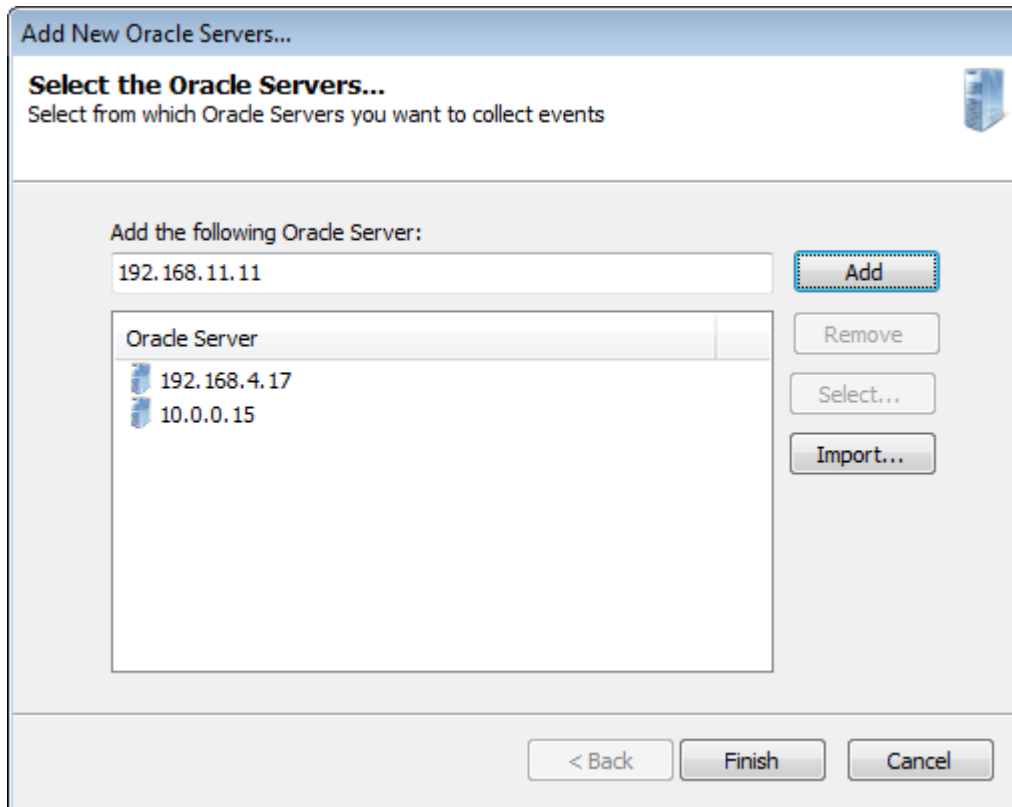
OPTION	DESCRIPTION
Archive all logs without further processing	Enable to archive events in the database backend without processing.
Process the logs with the rules selected below before archiving.	Select option to specify the rules to perform before archiving events in the database backend.

7. Click **OK**

6.6.3 Adding a new Oracle Server event source

To add a new Oracle Database to a database group:

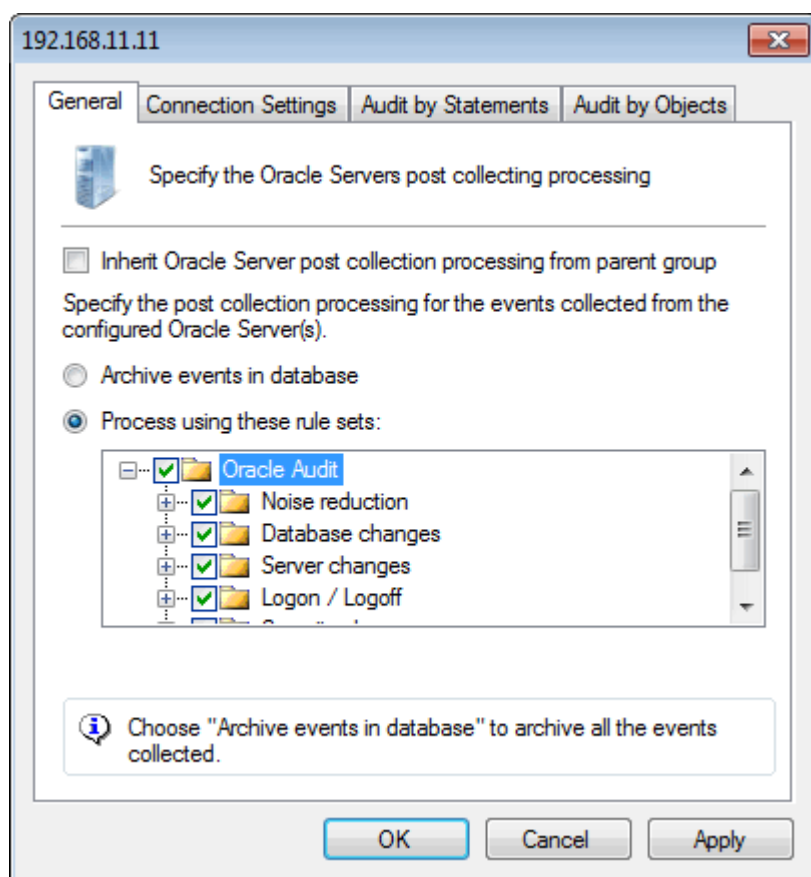
1. Right-click the database group and select **Add new Oracle Server**.



Screenshot 68 - Add new Oracle server

2. Key in the server name or IP and click **Add**. To import a server list from a text file, click **Import** and locate the text file.

Click Configuration ► Event Sources and from the Group Type, select Database Servers Groups.



Screenshot 69 - Oracle Database - General tab

3. From **Groups**, select **Oracle Servers**. Double-click the Oracle Database instance from the right pane and configure the options described below:

Table 48 - Oracle Database - General tab options

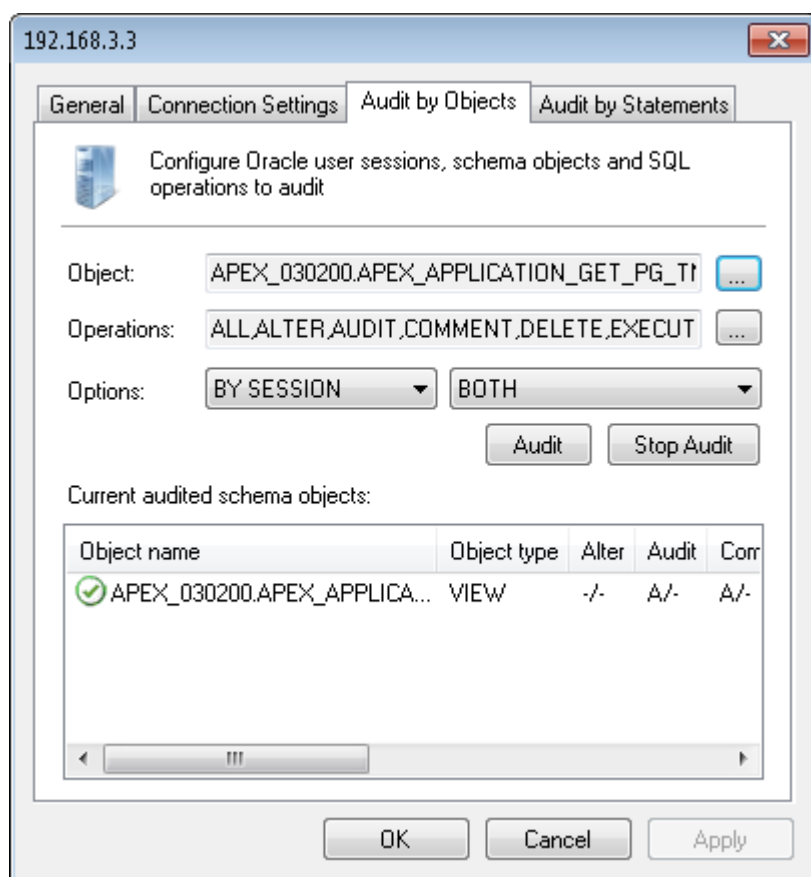
OPTION	DESCRIPTION
Inherit Oracle Server post collecting processing from parent group.	Select to inherit all settings from the parent group.
Archive events in database	Archive all events in the database backend without processing.
Process using these rule sets	Archive all events using the specified rules. Select the rules to apply.

Screenshot 70 - Oracle Database - Connection Settings tab

5. Select **Connection Settings** and configure the options described in the table below

Table 49 - Oracle Database - General tab options

OPTION	DESCRIPTION
Inherit the logon credentials from the parent group	Select to inherit login settings from the parent group.
Port	Key in the port to use to connect to the Oracle Database.
SID	The SID is a unique name to identify an Oracle Database instance. Key in the SID of the database to audit.
Service Name	The Service name is the alias used to identify the Oracle Database. Key in the Service name of the database to audit.
Test	Test the connection with the Oracle Database server.

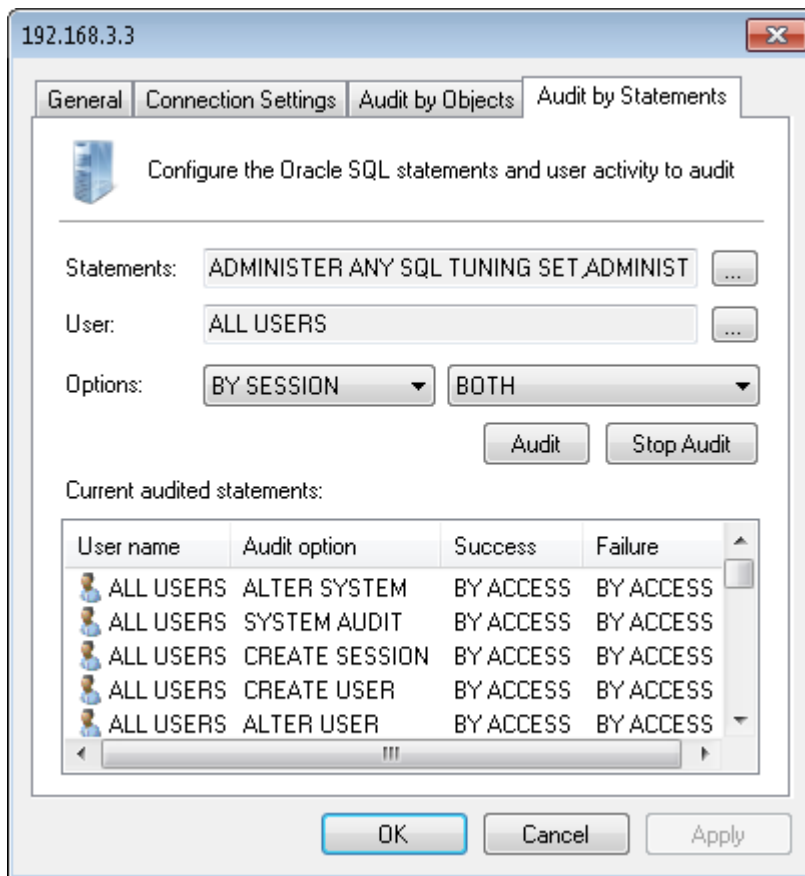


Screenshot 71 - Oracle Database - Audit by objects tab

6. Select **Audit by Objects** and configure the options described in the table below:

Table 50 - Oracle Database - Audit by Objects

OPTION	DESCRIPTION
Object	Click Browse to launch a list of available Oracle SQL objects. Select the object to audit and click OK . NOTE: Amongst others, Oracle objects can be procedures, views, functions and tables.
Operations	Operations are actions that modify or query an object. Click Browse to launch a list of available operations. Select the operations to audit and click OK .
Options	Select the audit options: <ul style="list-style-type: none"> » By Access - Creates an audit log per object operation execution. » By Session - Creates an audit log per operation and per schema object. A session is the time between a connection and a disconnection to/from the database. » Success - Select to process only successful audits. » Failure - Select to process only failed audits. Oracle will create an audit log if an audit fails to complete. » Both - Select to process all audit logs.
Audit	Choose this option to instruct the Oracle server to start auditing the server activities corresponding to the selected parameters (like users, statements, etc.)
Stop Audit	Choose this option to instruct the Oracle server to stop auditing the server activities corresponding to the selected parameters (like users, statements, etc.)
Current audited schema objects	A list that displays all current Oracle audited schema.



Screenshot 72 - Oracle Database - Audit by statements tab

7. Select **Audit by Statements** and configure the options described in Table 51 below.

Table 51 - Oracle Database - Audit by Statements

OPTION	DESCRIPTION
Statements	Click browse button to launch a list of available SQL statements. Select the SQL statements to audit and click OK . NOTE: Amongst others, Oracle statements can be ALTER, CREATE and SELECT SQL statements.
User	Oracle enables you to audit statements for a specific user. Click browse button to launch a list of available users. Select the user and click OK .
Options	Select audit options: <ul style="list-style-type: none"> » By Access - Creates one audit log for each statement execution. » By Session - Creates one audit log per user and per schema object. A session is the time between a connection and a disconnection to/from the database. » Success - Processes only successful audits. » Failure - Select option to process only failed audits. Oracle will create an audit log if an audit fails to complete. » Both - Select option to process all audit logs.
Audit	Choose this option to instruct the Oracle server to start auditing the server activities corresponding to the selected parameters (like users, statements, etc.)
Stop Audit	Choose this option to instruct the Oracle server to stop auditing the server activities corresponding to the selected parameters (like users, statements, etc.)
Current audited statements	A list that displays all current Oracle audited statements.

8. Click **OK**.

6.7 GFI LanGuard event sources

GFI EventsManager enables you to monitor events generated by GFI LanGuard. GFI LanGuard is a network vulnerability scanner that audits your network for weaknesses that can be exploited by users for malicious purposes. During network audits, GFI LanGuard creates events in the 'Application Log' of the machine where it is installed.

For each machine scanned by GFI LanGuard, an 'Application log' entry having 'Event ID: 0' and 'Source' set as GFI LanGuard will be generated. These events denote network vulnerability information extracted from scanned computers including:

INFORMATION GATHERED BY GFI LANGUARD	DESCRIPTION
Threat level	Gather information about the overall network threat level. This rating is generated through an extensive algorithm after GFI LanGuard audits the network
Missing patches and service packs	Find out which machines have missing updates and which updates need to be installed to strengthen the security level.
Open ports	Discover any unwanted open TCP and/or UDP ports.
Antivirus operational and malware definition status	GFI LanGuard is able to check if your virus database definitions are up to date. If it is not, you will be alerted and GFI LanGuard will attempt to update it.
Applications detected on scanned targets	GFI LanGuard enumerates applications installed on scan targets. You can create an inventory of wanted and/or unwanted applications and configure GFI LanGuard to automatically uninstall applications categorized as unwanted.



For more information about GFI LanGuard, refer to <http://www.gfi.com/network-security-vulnerability-scanner>.

Event 0, GFI LANguard

General

Details

```
<?xml version="1.0"?>
<LANguardEvent xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <computer><![CDATA[LUCIMAIN]]></computer>
  <highVulnerabilities>30</highVulnerabilities>
  <mediumVulnerabilities>21</mediumVulnerabilities>
  <lowVulnerabilities>13</lowVulnerabilities>
  <potentialVulnerabilities>1</potentialVulnerabilities>
  <missingServicePacks>1</missingServicePacks>
  <missingPatches>2</missingPatches>
  <openTCPDangerousPorts>0</openTCPDangerousPorts>
  <openUDPDangerousPorts>0</openUDPDangerousPorts>
  <passwordMinimumLength>0</passwordMinimumLength>
  <passwordMinimumAge>0</passwordMinimumAge>
  <passwordMaximumAge>3628800</passwordMaximumAge>
  <installedApplications>192</installedApplications>
  <unauthorizedApplications>0</unauthorizedApplications>
  <antivirusApplications>1</antivirusApplications>
  <antivirusApplicationsUpToDate>0</antivirusApplicationsUpToDate>
  <passwordForceLogoff><![CDATA[-1]]></passwordForceLogoff>
  <passwordHistoryStr><![CDATA[0]]></passwordHistoryStr>
  <successAudit>-1</successAudit>
  <failureAudit>-1</failureAudit>
  <topTenVulnerabilities>
    <string><![CDATA[All Servers: Brian Stanback bslist.cgi]]></string>
    <string><![CDATA[OVAL:7191: Adobe Flash Player and AIR 'exception_count' Integer Overflow Vulnerability]]></string>
    <string><![CDATA[OVAL:7465: Adobe Flash Player and AIR JPEG File Parsing Heap Buffer Overflow Vulnerability]]></string>
    <string><![CDATA[OVAL:7460: Adobe Flash Player and AIR Data Injection Remote Code Execution Vulnerability]]></string>
    <string><![CDATA[OVAL:7140: Adobe Flash Player and AIR Unspecified Memory Corruption Vulnerability]]></string>
    <string><![CDATA[OVAL:7011: Adobe Flash Player and AIR NULL Pointer Exception Remote Code Execution Vulnerability]]></string>
    <string><![CDATA[OVAL:6998: Adobe Flash Player and AIR 'intf_count' Integer Overflow Vulnerability]]></string>
    <string><![CDATA[OVAL:6972: Adobe Flash Player and AIR Multiple Unspecified Remote Code Execution Vulnerabilities]]></string>
    <string><![CDATA[OVAL:6961: Adobe Flash Player and AIR Unspecified Privilege Escalation Vulnerability]]></string>
    <string><![CDATA[OVAL:6899: Adobe Flash Player and AIR Unspecified Memory Corruption Vulnerability]]></string>
  </topTenVulnerabilities>
</LANguardEvent>
```

Log Name:

Application

Source:

GFI LANguard

Logged:

8/27/2010 3:29:45 PM

Event ID:

0

Task Category:

None

Level:

Information

Keywords:

Classic

User:

N/A

Computer:

LuciMain

OpCode:

More Information:

[Event Log Online Help](#)

Screenshot 73 - Event generated by GFI LanGuard



GFI EventsManager can process events generated by GFI LanGuard version 9.5 or later.

6.7.1 How to enable GFI LanGuard event logging?

To start monitoring 'Application log' entries generated by GFI LanGuard:

1. Add the machine where GFI LanGuard is installed as an event source.



For information, refer to [Manage event sources](#).

2. Once GFI LanGuard machine is added as an event source, GFI EventsManager will remotely and automatically enable the event logging feature in GFI LanGuard by creating and setting the following registry value on the GFI LanGuard machine:

```
HKEY_LOCAL_MACHINE\SOFTWARE\GFI\LNSS[n]\Config\EventLog = 1  
(dword)
```



[n] is the major version number of GFI LanGuard.

Example: `HKEY_LOCAL_MACHINE\SOFTWARE\GFI\LNSS9\Config\EventLog = 1 (dword)`



To stop GFI LanGuard from generating 'Application Log' entries, remove the registry value described above or change the registry value to 0.

6.7.2 Monitoring GFI LanGuard Events

GFI EventsManager has built-in processing rules for GFI LanGuard events that are enabled by default. To monitor events generated by GFI LanGuard, select **Status** tab ► **General** and locate the **Critical and High Importance Events** section.



To configure GFI LanGuard event processing rules, click **Configuration** tab ► **Event Processing Rules** and from the left pane select **GFI Rules** ► **GFI LanGuard rules**. For more information, refer to [Using event processing rules](#).

6.8 GFI EndPointSecurity event sources

GFI EndPointSecurity enables you to maintain data integrity by preventing unauthorized access and transfer of content to and from the following devices or connection ports:

DEVICE	EXAMPLE
USB Ports	Flash/Memory card readers and pen drives.
Firewire ports	Digital cameras and Fire-wire card readers.
Wireless devices	Bluetooth and Infrared dongles
Floppy disk drives	Internal and external (USB) floppy drives.
Optical drives	CD, DVD and Blu-ray discs.
Magneto Optical drives	Internal and external (USB) drives.
Removable storage	USB hard-disk drives.
Other drives such as Zip drives and tape drives	Internal or External (USB/Serial/Parallel) drives.



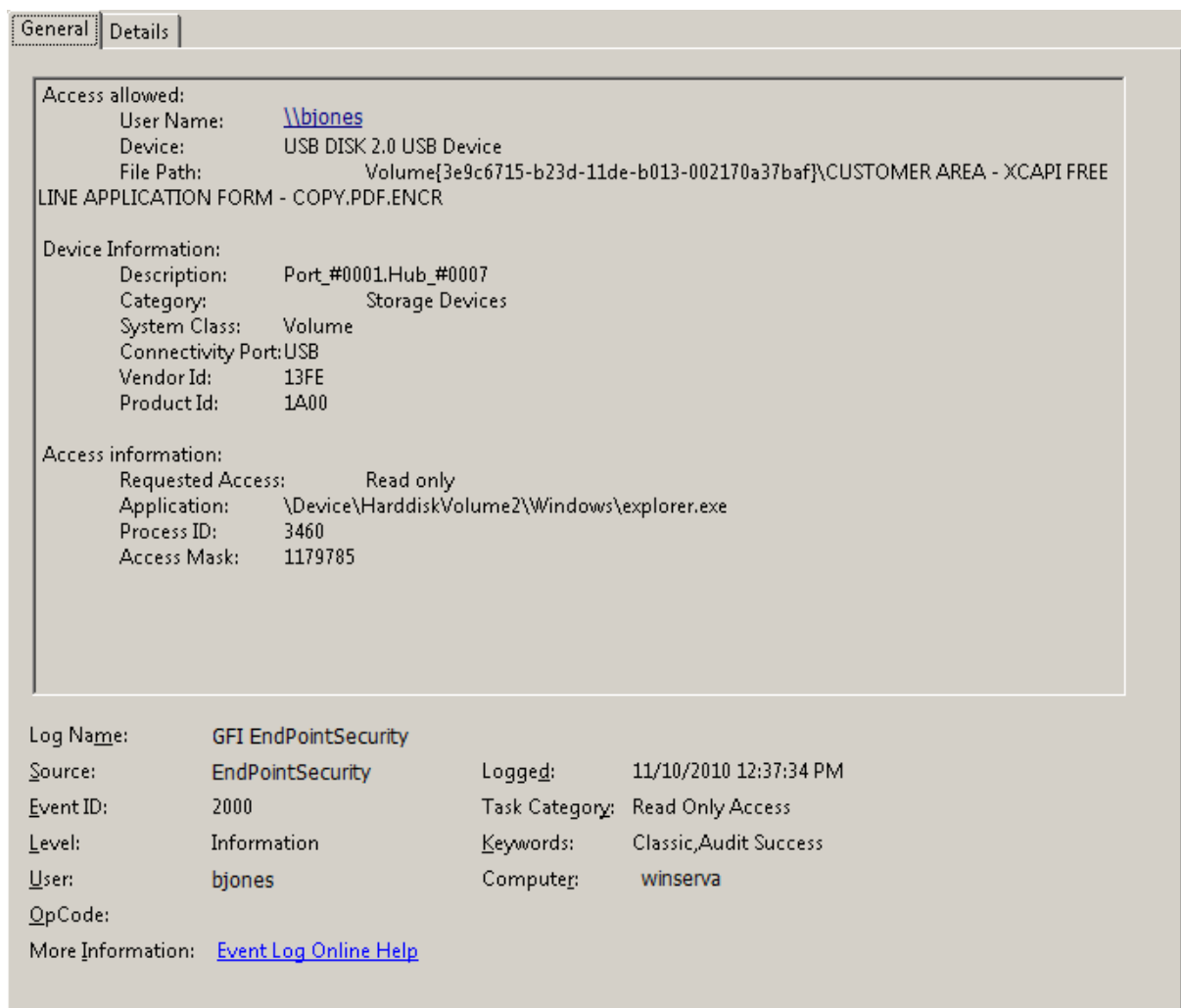
For more information about GFI EndPointSecurity, refer to <http://www.gfi.com/endpointsecurity>

6.8.1 Enable GFI EndPointSecurity logging

By default, GFI EndPointSecurity generates logs with information about:

- » The GFI EndPointSecurity service

- » Devices connected and disconnected on your network
- » Access allowed or denied by GFI EndPointSecurity to users.



Screenshot 74 - Event generated by GFI EndPointSecurity

To configure the logging options in GFI EndPointSecurity:

1. From the GFI EndPointSecurity machine, launch GFI EndPointSecurity management console.
2. Click Configuration tab ► Protection Policies.
3. From the left pane, select the protection policy and click **Set Logging Options**.
4. Customize the settings available in **Logging Option** dialog.



For more information on how to configure GFI EndPointSecurity logging options, refer to the GFI EndPointSecurity documentation available from <http://www.gfi.com/products/gfi-endpointsecurity/manual>.

6.8.2 Monitor GFI EndPointSecurity Events

GFI EventsManager has built-in processing rules for GFI EndPointSecurity events that are enabled by default. To monitor events generated by GFI EndPointSecurity, select **Status** tab ► **General** and locate the **Critical and High Importance Events** section.

To configure GFI EndPointSecurity event processing rules, click **Configuration** tab ► **Event Processing Rules**. For more information, refer to [Using event processing rules](#).

7 Using event processing rules

7.1 Introduction

This chapter includes sections containing information about:

- » Collecting Windows events
- » Collecting W3C logs
- » Collecting Syslogs
- » Collecting SNMP Traps
- » Collecting custom events
- » Triggering a manual event source scan

GFI EventsManager allows you to collect and process: Windows Event Logs, W3C logs, Syslogs, SNMP Traps and Microsoft SQL Server audit logs. All supported log types record events in a different and proprietary format; therefore every log type requires different configuration settings and parameters. You can configure log collection and processing parameters:

- » On a computer by computer basis
- » On a computer group by computer group basis.

During event processing, GFI EventsManager runs a configurable set of rules against the collected logs in order to classify events and trigger alerts/actions accordingly. By default, GFI EventsManager ships with a pre-configured set of event processing rules that allow you to gain network-wide control over computer logs - with negligible configuration effort.

7.1.1 Event processing rules

EVENT PROCESSING RULES ARE INSTRUCTIONS/CHECKS THAT:

Analyze the collected logs.

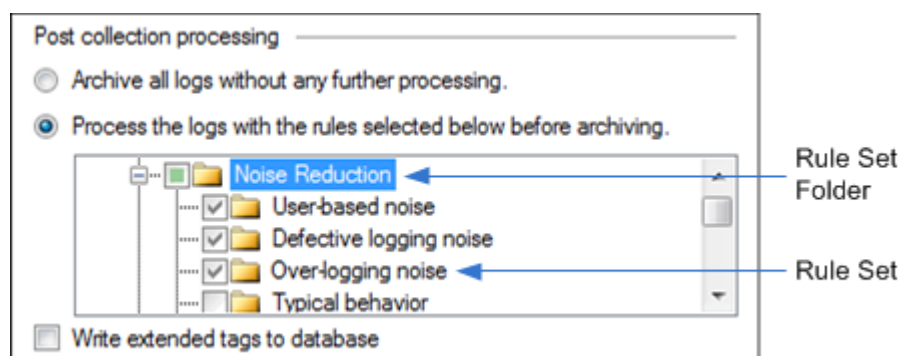
Classify the severity of processed events. Classification is based on the configuration settings of the processing rule.

Filter events that match specific criteria. Example: you can create and run a rule which filters out low severity events and noise (duplicate events).

Generate alerts and actions based on event severity. Example: you can configure GFI EventsManager to send both SMS and Email alerts whenever an event is classified as critical; but limit the product to send only email alerts when an event is classified as high in severity. For more information, refer to [Configuring alerting options](#).

Optionally archive filtered events. Event archiving is based on the severity of the event and on the configuration settings of the event processing rules. Example: you can configure GFI EventsManager to archive only events that are classified as critical or high in severity and discard all the rest.

In GFI EventsManager, event processing rules are organized into 'Rule-sets'; and every rule-set can contain one or more specialized rules which can be run against collected logs.



Screenshot 75 - Rule-sets folder and Rule-sets

Rule-sets are further organized into **Rule-sets Folders**. This way you can group rule-sets according to the functions and actions that the respective rules perform. By default, GFI EventsManager ships with pre-configured folders, rule-sets and event processing rules that can be further customized to suite your event processing requirements.

7.1.2 Event classification

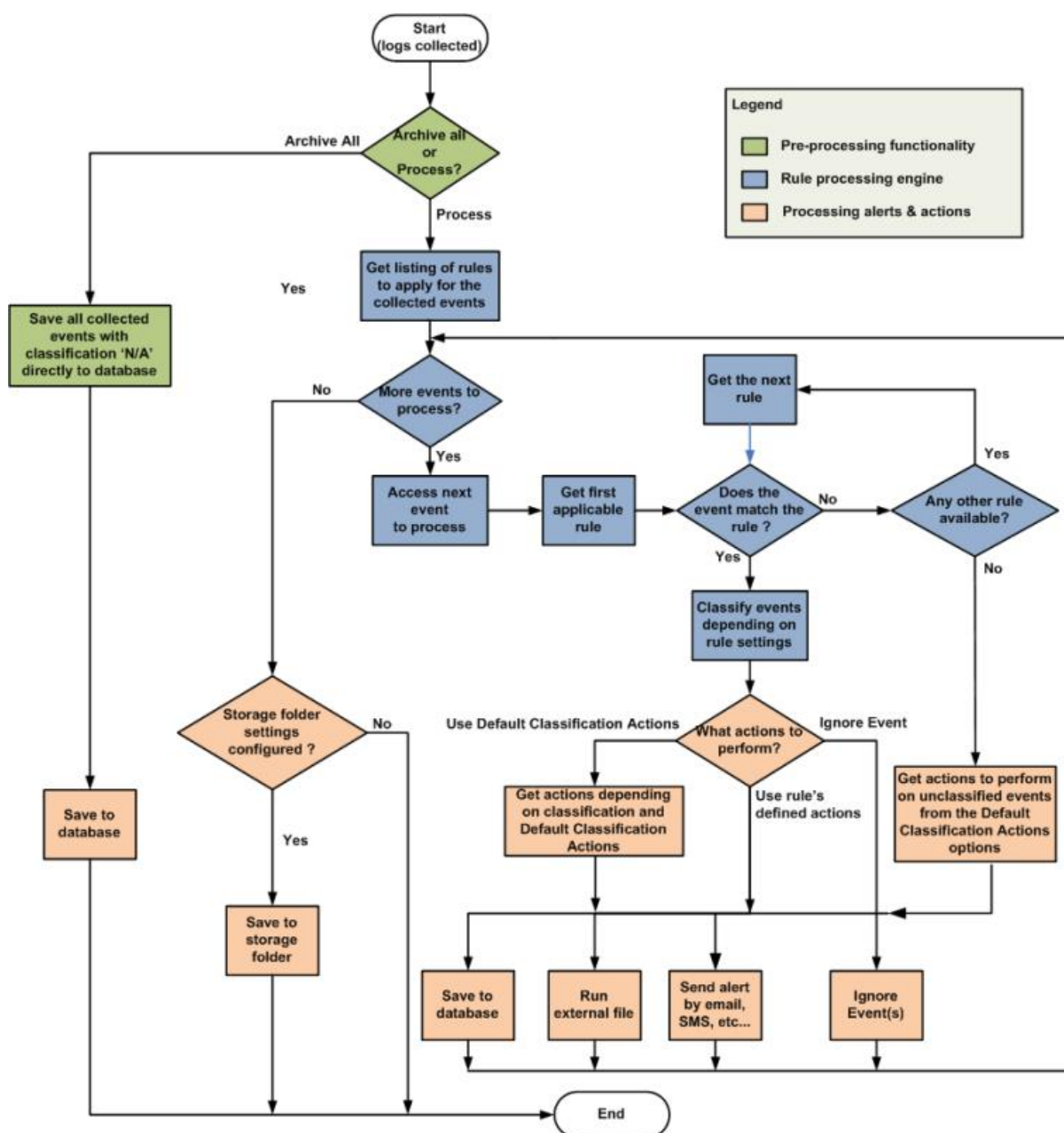
Event classification is based on the configuration of the rules that are executed against the collected logs. Events that don't satisfy any event classification conditions are tagged as unclassified. Unclassified events may also be used to trigger the same alerts and actions available for classified events.

GFI EventsManager classifies events in the following categories:

- » Critical
- » High
- » Medium
- » Low
- » Noise (unwanted or repeated log entries).

7.1.3 How event processing works

The flowchart chart below illustrates the event processing stages performed by GFI EventsManager.



Screenshot 76 - Log processing, classification and actions flowchart

7.2 Collecting Windows events

Windows events are organized into specific log categories; by default computers running on Windows NT or higher, record errors, warnings and information events in three logs namely Security, Application and System logs.

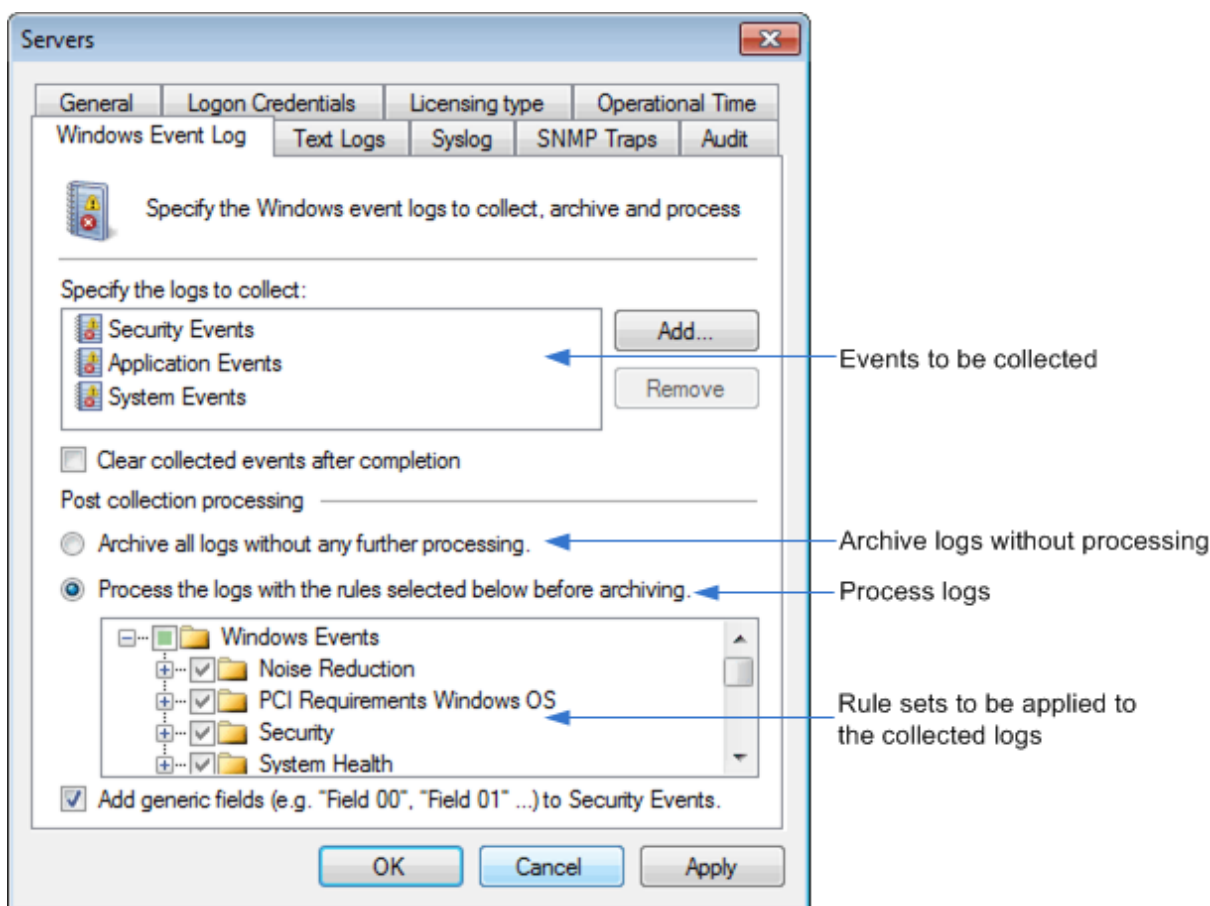
Computers that have more specialized roles on the network such as Domain Controllers, and DNS Servers have additional event log categories.

As a minimum, Windows Operating Systems record events in the following logs:

Table 52 - Windos Event Logs collected by GFI EventsManager

LOG TYPE	DESCRIPTION
Security event log	This log contains security related events through which you can audit successful or attempted security breaches. Typical events found in the Security Events log include valid and invalid logon attempts.
Application event log	This log contains events recorded by software applications/programs such as file errors.
System event log	This log contains events logged by operating system components such as failures to load device drivers.

LOG TYPE	DESCRIPTION
Directory service log	This log contains events generated by the Active Directory including successful or failed attempts to make to update the Active Directory database.
File Replication service log	This log contains events recorded by the Windows File Replication service. These including file replication failures and events that occur while domain controllers are being updated with information about Sysvol.
DNS server log	This log contains events associated with the process of resolving DNS names to IP addresses.
Application and Services Logs	These logs contain events associated with Windows VISTA and the relative services/functionalities it offers.



Screenshot 77 - Computer group properties: Configuring Windows Event Logs parameters

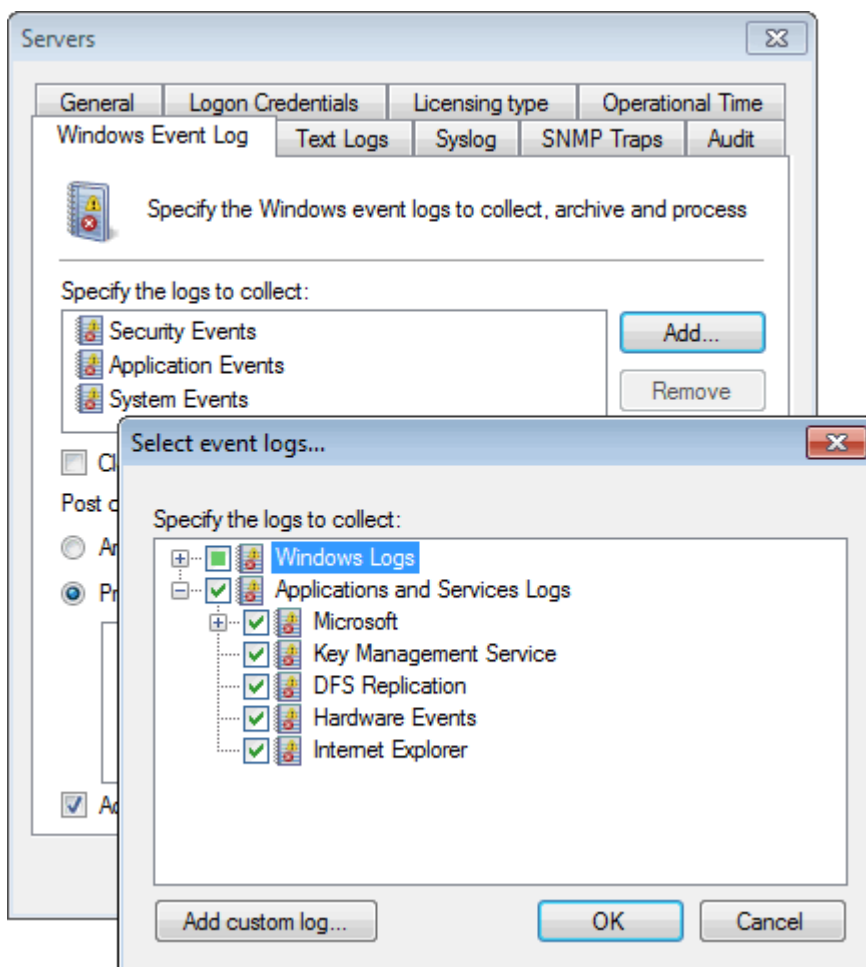
To configure Windows Event Log collection and processing parameters:

1. From **Configuration** tab ► **Event Sources**, right-click an event source group and select **Properties**.
2. Click **Windows Event Log** and configure the parameters described below:

Table 53 - Configuring Windows Event Log processing

OPTION	DESCRIPTION
Specify the logs to collect	Click Add to select the Windows Logs and/or Applications and Services Logs to collect. You can also add custom logs to be collected by event sources in this group. For information, refer to Collecting custom events .
Clear collected events after completion	(Optional) Select this option to clear the collected events from event sources, after they have been processed.
Archive all logs without any further processing	Select this option to archive the process W3C logs without applying further checks.

OPTION	DESCRIPTION
Process the logs with the rules selected below, before archiving	Select this option and select the events processing rules you want to run against the collected events.
Write extended tags to database	Add extended fields to the database. Extended fields contain data from event descriptions and are added by a common name.



Screenshot 78 - Selecting the events to be collected

3. Click **OK** to finalize your settings.



Deleting event logs without archiving may lead to legal compliance issues.

7.3 Collecting Text logs

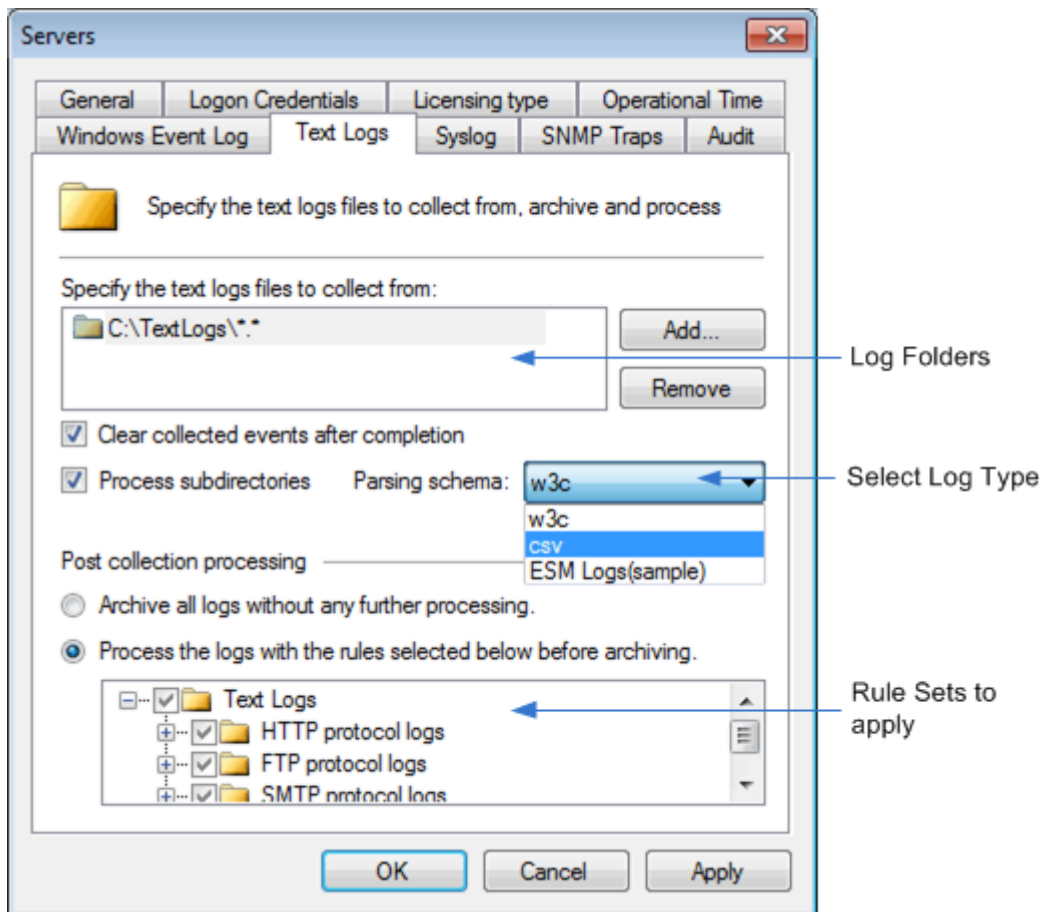
W3C is another log format supported by GFI EventsManager. W3C logs are text-based flat files containing various event details delimited by special characters.

The W3C log format is mostly commonly used by hardware systems (Example: servers and appliances) which have internet specific roles. Microsoft Internet Information Server (IIS) service and Apache web servers for example, can collect web related events such as web logs, in the form of W3C formatted text files.

In GFI EventsManager, the configuration process of W3C log parameters is identical to that performed for Windows event processing, with one exception. Unlike Windows Event Logs, there is no standard which dictates a specific or centralized folder location where W3C log files are stored on disk. Therefore, in order to collect W3C logs, you must specify the complete path to these text-based log files.

To configure W3C log collection and processing parameters:

1. From **Configuration** tab ► **Event Sources**, right-click an event source group and select **Properties**.



Screenshot 79 - Computer group properties: Configuring W3C event processing parameters

2. Click **Text Logs** and configure the options described below:

Table 54 - Configuring W3C processing

OPTION	DESCRIPTION
Specify the files in W3C format to collect	Click Add to specify the log file name and location. Wildcards such as *. * are supported.
Clear collected events after completion	Select this option to clear events collected from event sources.
Process subdirectories	This option enables you to recursively scan the specified path that contains W3C logs.
Parsing schema	Select the schema in which W3C logs are interpreted. Select from: <ul style="list-style-type: none"> » W3C » CSV » EMS Logs.
Archive all logs without further processing	Select this option to archive the processed W3C logs without applying further checks.
Process the logs with the rules selected below, before archiving	Select additional checks to run against collected W3C logs.

3. Click **OK** to finalize your settings.



Deleting event logs without archiving may lead to legal compliance issues.

7.4 Collecting Syslogs

Syslog is a data logging service that is most commonly used by Linux and UNIX based systems. The concept behind Syslogs is that the logging of events and information is entirely handled by a dedicated server called 'Syslog Server'.

Unlike Windows and W3C log based systems, Syslog enabled devices send events in the form of data messages (technically known as 'Syslog Messages') to a Syslog server that interprets and manages message and saves the data in a log file.

In order to process Syslog messages, GFI EventsManager ships with a built-in Syslog Server. This Syslog server will automatically collect, in real-time, all Syslog messages/events sent by Syslog sources and pass them on to the event processing engine. Out-of-the-box, GFI EventsManager supports events generated by various network devices manufactured by leading providers including Cisco and Juniper.



For more information about supported devices visit:

<http://kbase.gfi.com/showarticle.asp?id=KBID002868>.



A built-in buffer allows the Syslog server to collect, queue and forward up to 30 Syslog messages at a time. Buffered logs are by default passed on to the event processing engine as soon as the buffer fills up or at one minute intervals; whichever comes first.

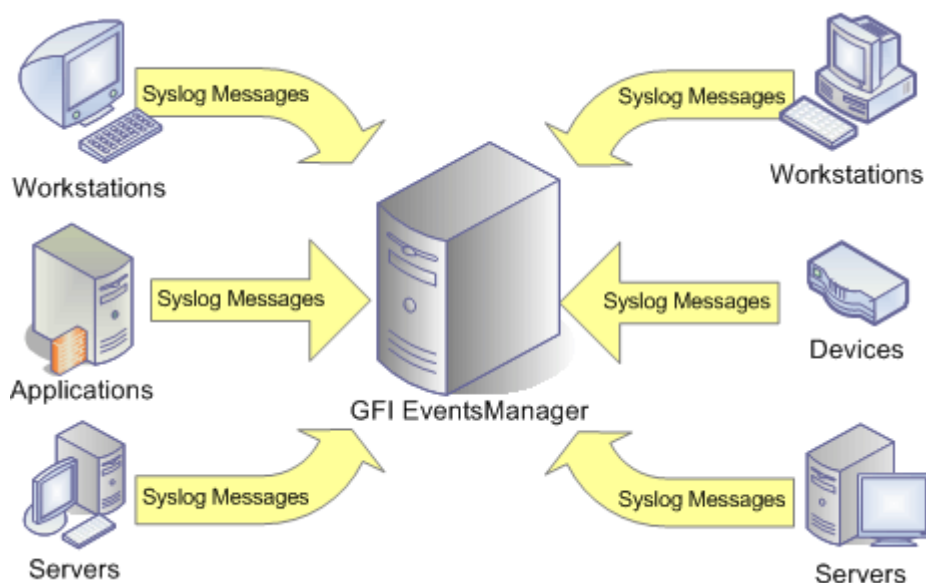


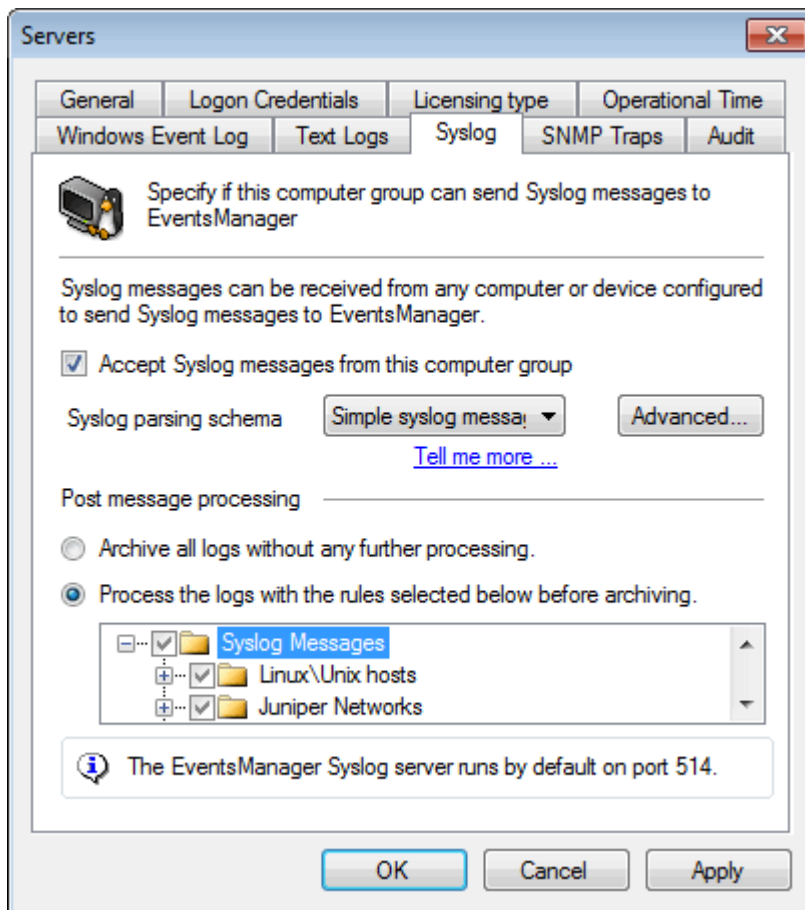
Figure 7 - Syslog messages must be directed to the computer running GFI EventsManager

To collect Syslog Messages:



Before you start collecting Syslogs, every Syslog event source (workstations, servers and/or network devices) must be configured to send their Syslog Messages to the computer name or IP where GFI EventsManager is installed.

1. From Configuration tab ► Event Sources, right-click an event source group and select Properties.



Screenshot 80 - Computer group properties: Syslog processing parameters

2. Click **Syslog** tab and configure the options described below:

Table 55 - Configuring Syslog processing

OPTION	DESCRIPTION
Accept Syslog messages from this computer group	Select this option to enable syslog message processing.
Syslog parsing schema	Select the method that GFI EventsManager Syslog Server interprets Syslog Messages from network devices. Select from: <ul style="list-style-type: none"> » Simple syslog message » Standard Linux message » Juniper Network Firewall » Cisco ASA.
Advanced...	Click Advanced... to use custom windows code page. Specify the code and click OK . Windows code page is used to encode international characters to ASCII strings. Since Syslog is not Unicode compliant, GFI EventsManager uses a code page to decode the events. This is only applicable if GFI EventsManager is installed on a machine using a different language than the monitored machines. For more information, refer to http://www.microsoft.com/globaldev/reference/wincp.msp
Archive all logs without any further processing	Select this option to archive the processed Syslogs without applying further checks.
Process the logs with the rules selected below, before archiving	Select additional checks to run against collected Syslogs.

3. Click **OK** to finalize your settings.

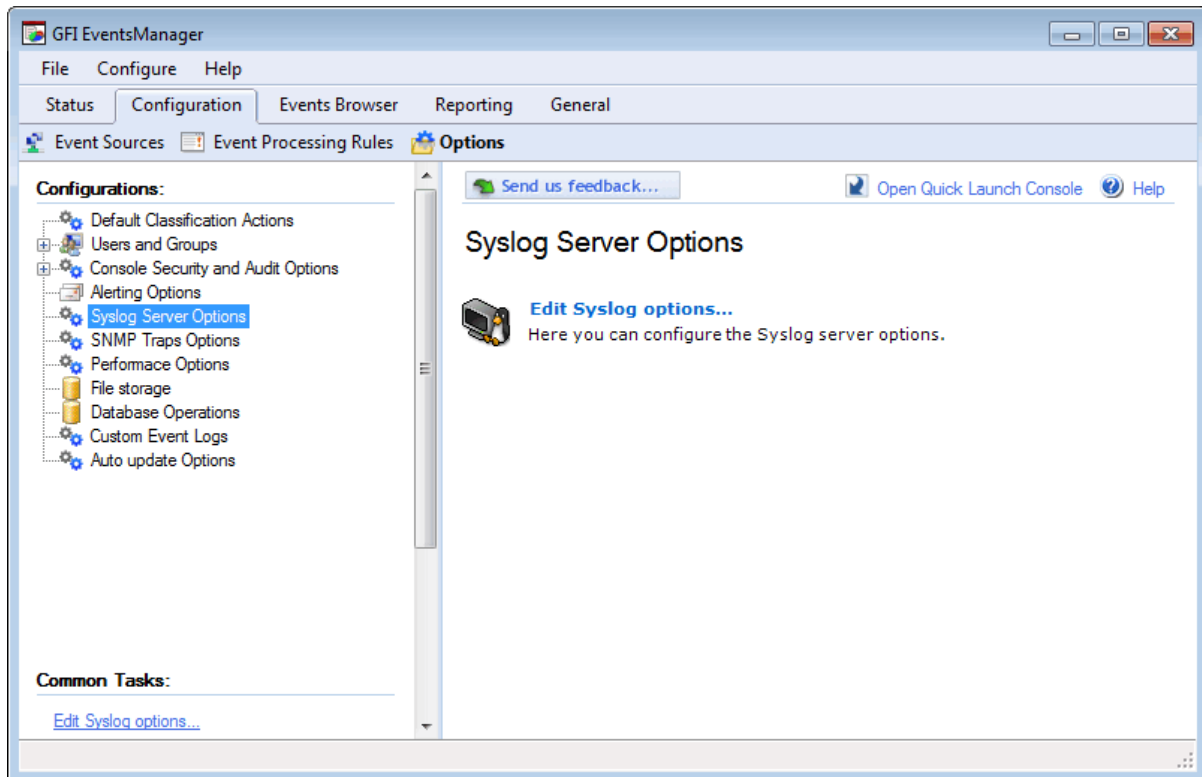


The GFI EventsManager Syslog server is by default configured to listen for Syslog messages on port 514. For more information on how to customize Syslog server port settings refer to [Configuring the Syslog server communications port](#) section in this chapter.



Deleting event logs without archiving may lead to legal compliance issues.

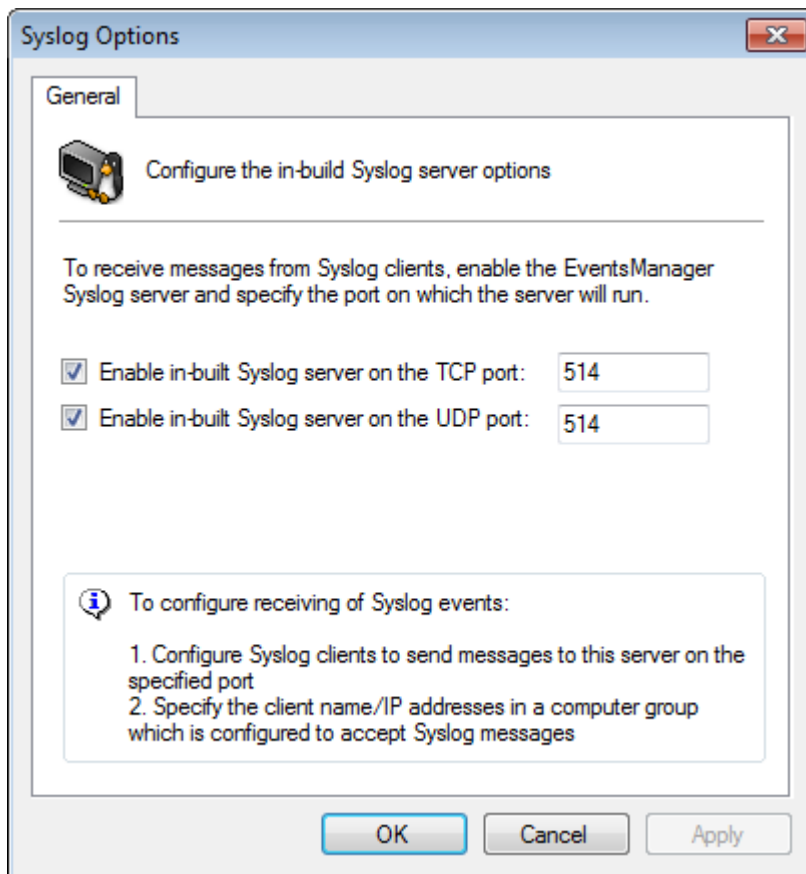
7.4.1 Configuring the Syslog server communications port



Screenshot 81 - Configuring Syslog Servercommunication port

To change the default Syslog ports settings:

1. Click **Configuration** tab ► **Options**.
2. Right-click **Syslog Server Options** and select **Edit Syslog options...**



Screenshot 82- Syslog server options

4. Select **Enable in-built Syslog server on TCP port:** and specify the TCP port on which GFI EventsManager will receive/listen for Syslog messages.
5. Select **Enable in-built Syslog server on UDP port:** and specify the UDP port on which GFI EventsManager will receive/listen for Syslog messages.
5. Select **OK** to finalize settings.



When configuring Syslog server port settings, make sure that the configured port is not already in use by other installed applications. This may affect the delivery of Syslog messages to GFI EventsManager.

7.5 Collecting SNMP Traps

SNMP is a data logging service that enables networked devices to log events and information through data messages (technically known as SNMP Traps). SNMP messaging technology is similar in concept to Syslogs - where unlike Windows and W3C log based environments, devices that generate SNMP messages do not record events data in local logs. Instead events information is sent in the form of data messages to an SNMP Trap Server which manages and saves SNMP message data in a local (centralized) log file.

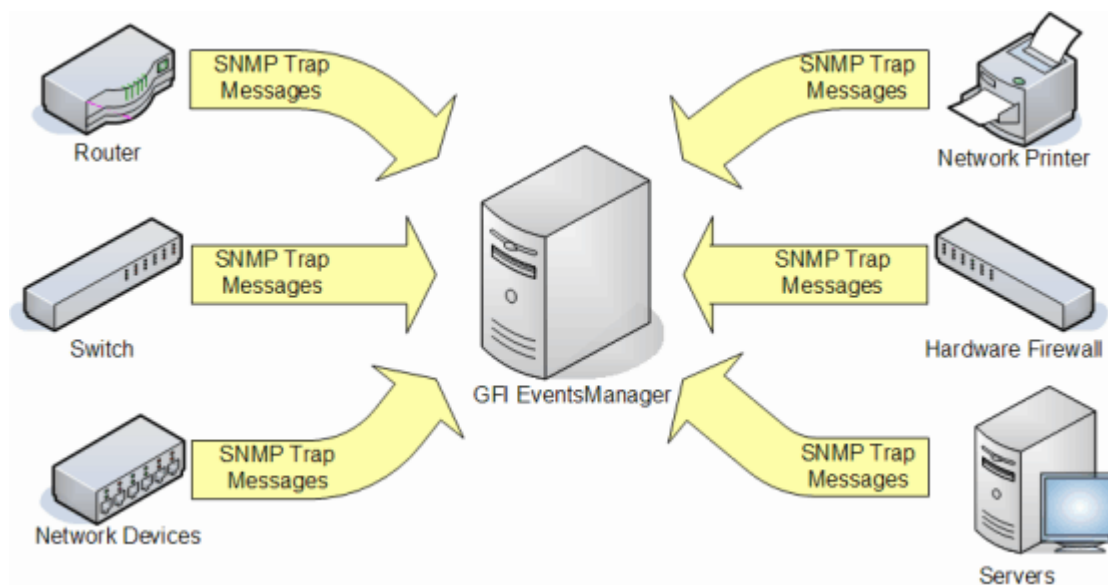


Figure 8: SNMP Trap messages must be directed to the computer running GFI EventsManager



GFI EventsManager natively supports an extensive list of SNMP devices and Management Information Bases (MIBs).

For a full list of supported devices visit:

<http://kbase.gfi.com/showarticle.asp?id=KBID002868>.

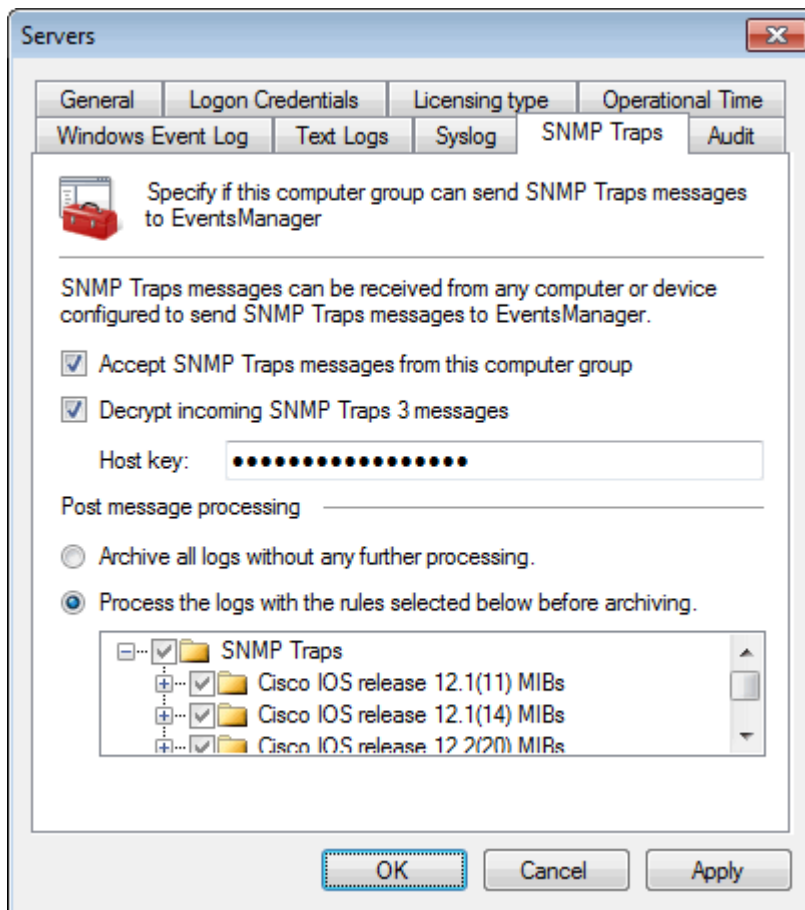
GFI EventsManager includes a dedicated SNMP Trap Server through which SNMP Traps are handled. A built-in buffer allows the SNMP Trap Server to collect, queue and forward up to 30 SNMP Trap at a time. Buffered logs are by default passed on to the event processing engine as soon as the buffer fills up or at one minute intervals; whichever comes first.

To collect SNMP Traps:



Before you start collecting SNMP Traps messages, every SMP event source (workstations, servers and/or network devices) must be configured to send their SNMP Traps Messages to the computer name or IP where GFI EventsManager is installed.

1. From Configuration tab ► **Event Sources**, right-click an event source group and select **Properties**.



Screenshot 83 - Computer group properties: SNMP processing parameters

2. Click **SNMP Traps** tab and configure the options described below:

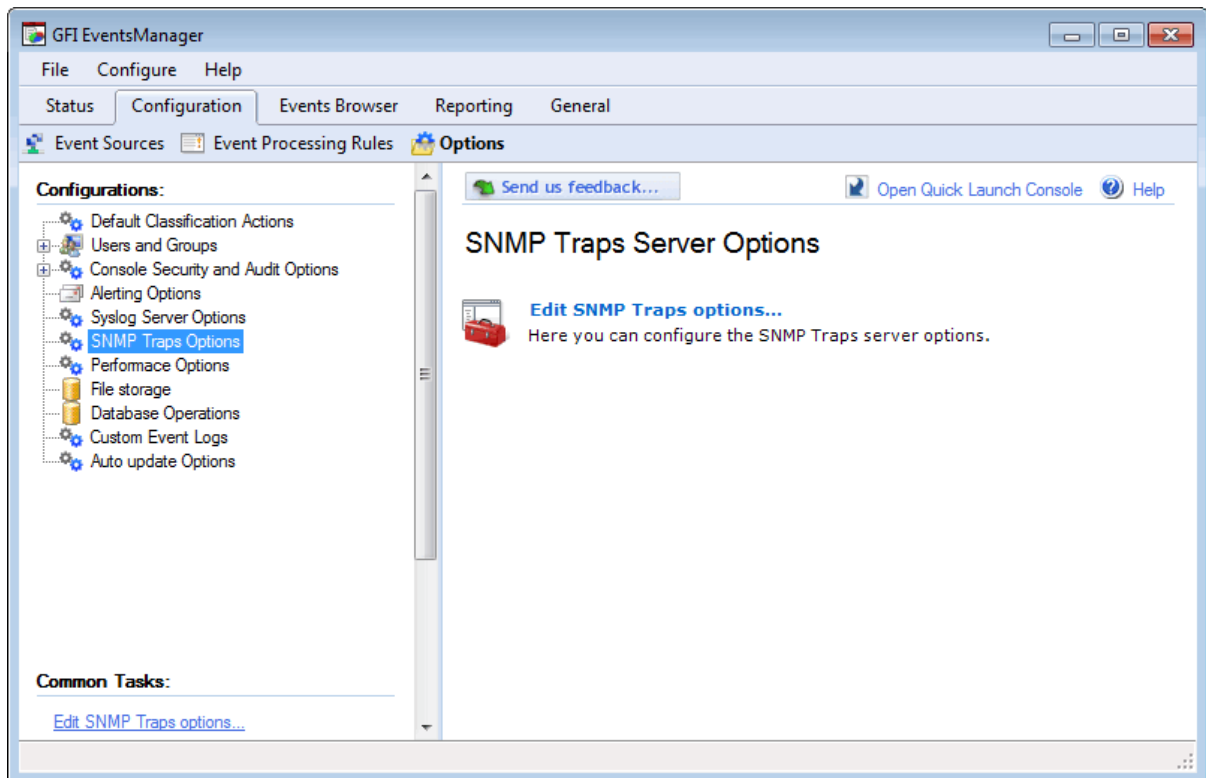
Table 56 - Configuring SNMP Traps processing

OPTION	DESCRIPTION
Accept SNMP Traps messages from this computer group	Select this option to enable SNMP Traps messages processing.
Decrypt incoming SNMP Traps 3 messages	This option enables you to decrypt SNMP Traps 3 messages.
Host key	If Decrypt incoming SNMP Traps 3 messages is enabled, key in the decryption key in this field.
Archiving all logs without any further processing	Select this option to archive the processed SNMP Traps messages without applying further checks.
Process the logs with the rules selected below, before archiving	Select additional checks to run against collected SNMP Traps messages.

3. Click **OK** to finalize your settings.

	The GFI EventsManager SNMP Trap Server is by default configured to listen for SNMP Trap messages on port 162. For more information, refer to Configuring the SNMP Trap server settings .
	The built in SNMP Trap Server supports SNMP version 3 Traps with encryption. For encrypted SNMP messages the encryption host key must be provided in the decrypt incoming SNMP Traps 3 message field
	Deleting events from source logs without archiving may lead to legal compliance issues.

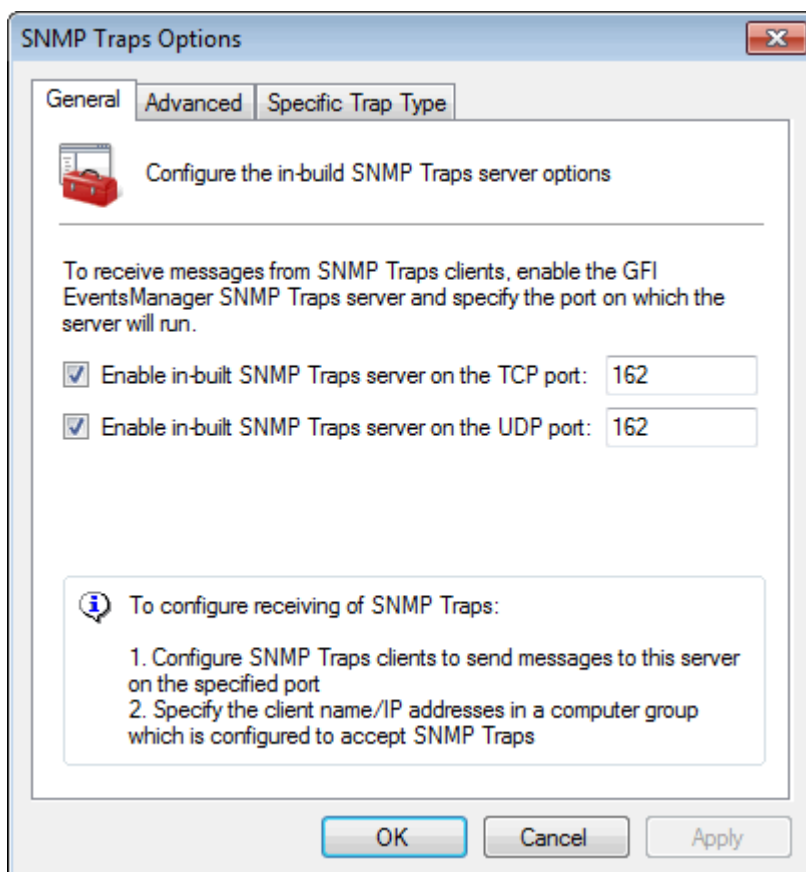
7.5.1 Configuring the SNMP Trap server



Screenshot 84 - Configuring SNMP Traps

To change the default SNMP Trap Server settings:

1. Click **Configuration** tab ► **Options**.
2. Right-click **SNMP Traps Options** and select **Edit SNMP Traps options...**



Screenshot 85- SNMP Traps options

3. Enable the required TCP/UDP SNMP server. Specify the TCP/UDP port on which GFI EventsManager will listen for SNMP messages.
4. Click **Advanced** tab to add, edit or remove SNMP Trap object identifiers (OIDs).
5. Click **Specific Trap Type** tab to add, edit or remove trap types.
6. Click **OK** to finalize settings.



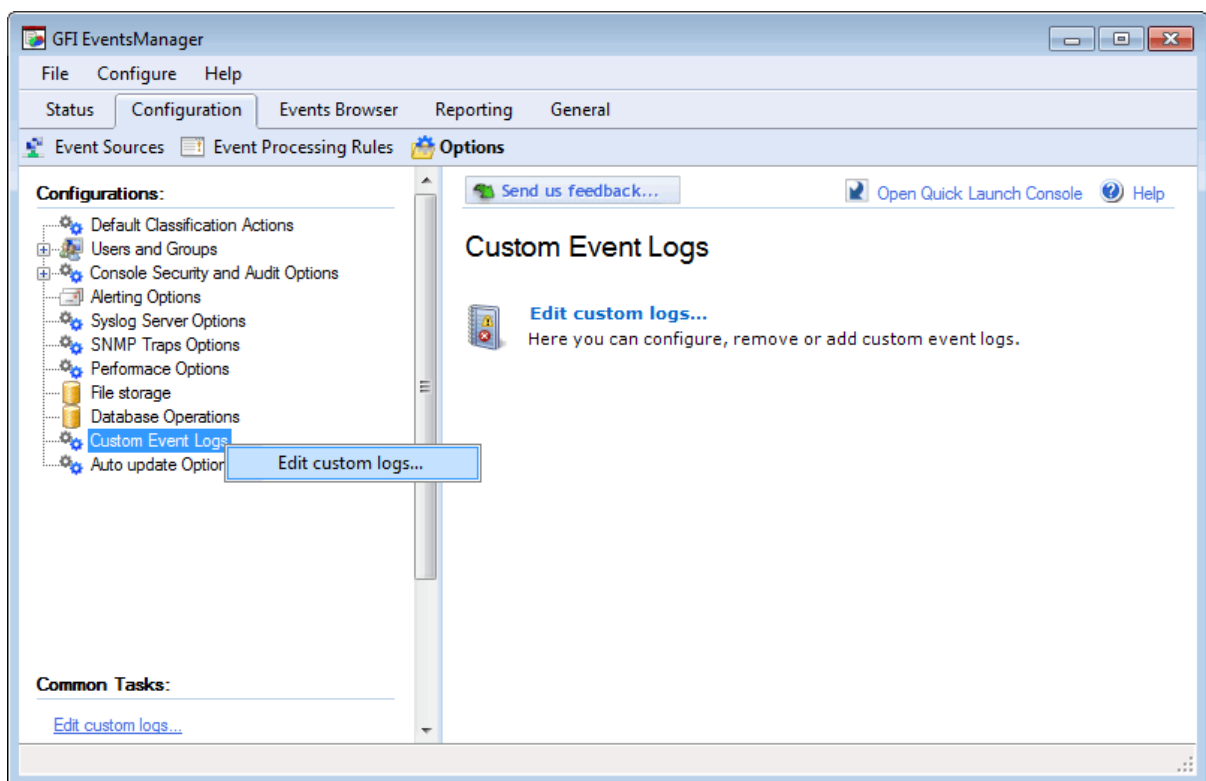
When configuring SNMP Trap Server port settings, make sure that the configured TCP or UDP port is not already in use by other installed applications. This may affect the delivery of SNMP Trap messages to GFI EventsManager.

7.6 Collecting custom events

GFI EventsManager is configured to collect and process standard event logs. However, GFI EventsManager can also be configured to manage events recorded in third party application logs such as anti-virus logs, software firewall logs and other security software.

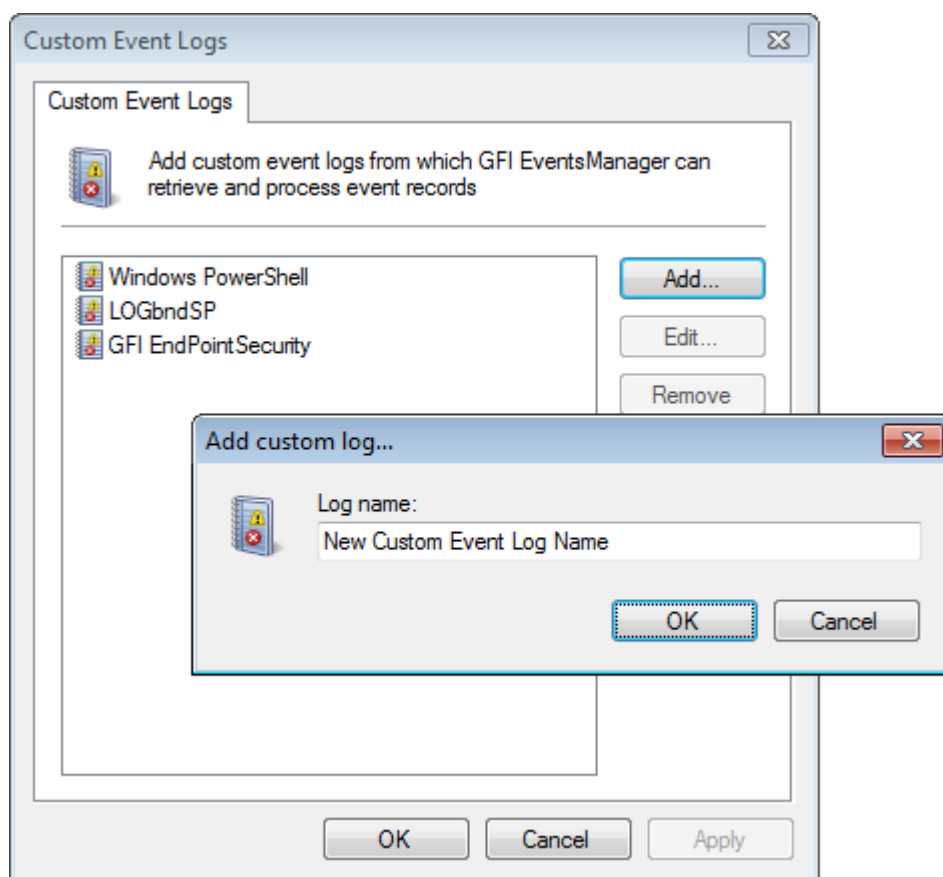
To configure custom events:

1. Click **Configuration** tab and select **Options**.



Screenshot 86 - Custom event logs setup

2. From **Configurations**, right-click **Custom Event Logs** and select **Edit custom logs...**



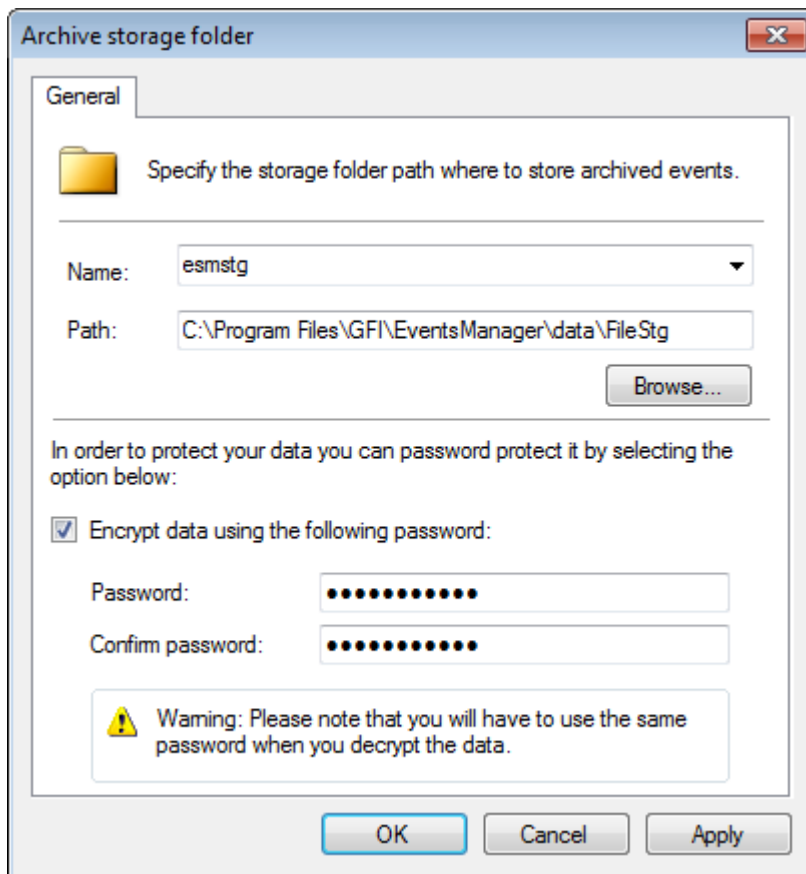
Screenshot 87 - Custom event logs dialog

3. Click **Add...** button and specify the name of your custom event log.
4. Click **OK** to finalize settings.
5. (Optional) Click **Edit** to rename the selected custom event, or click **Remove** to delete the selected custom event.

7.6.1 Configure storage folder

GFI EventsManager can be configured to archive events in a storage folder after applying processing rules. This feature allows the system to store all the events retrieved from event sources, on the local host (where GFI EventsManager is installed). To configure the storage folder:

1. Click **Configuration** tab ► **Options**.
2. From **Configurations**, right-click **Database and Files Backend** and select **Configure file storage...**



Screenshot 88 - Configure file storage dialog

3. Configure the options described below:

OPTION	DESCRIPTION
Name	Key in the name of the storage folder.
Path	Specify the path or browse for a storage folder.
Encrypt data using the following password	Select this option to securely encrypt the contents of the storage folder with a password.
Password / Confirm password	Specify the encryption password and confirm the specified password.

4. Click **OK** to finalize your settings.

7.7 Triggering a manual event source scan

In GFI EventsManager, you can manually trigger event collection iteration on target computers. To achieve this:

1. Right-click on a computer group or event source within a group.
2. Select Scanning options ► Scan now.

8 Manage rule-sets

8.1 Introduction

This chapter contains the following sections that will assist you in managing Event Processing Rules:

- » [Adding a rule-set folder](#)
- » [Creating new events processing rules](#)
- » [Creating a new rule from an existing event](#)
- » [Advanced event filtering parameters](#)

GFI EventsManager ships with pre-configured rule-sets that can be used to process events with minor configuration effort. You can also customize these default rules or create tailored ones for your organization's requirements. Events processing rules are conditions which:

Table 57 - Events Processing Rules

CONDITION	DESCRIPTION
Classify processed events	Configure GFI EventsManager to classify processed events. By default, events are categorized into five main categories; however, more categories may be added according to your requirements.
Filter out noise (repeated events) or unwanted events	GFI EventsManager is able to filter out unwanted events. This helps you maintain only wanted events and ignore unwanted noise.
Trigger email, SMS and network alerts on key events	Configure automated actions to run when specific events are processed. For more information, refer to Configuring Alerting Options .
Attempt remedial actions by executing specific scripts and executable files on key events	Run executable files, commands and/or scripts upon detecting a specified event and/or number of events.

In GFI EventsManager, event processing rules are organized into rule-sets, which in turn are stored in rule-set folders. The table below lists some of the most common rule-set folders in GFI EventsManager:

Table 58 - Rule-set folders available in GFI EventsManager

RULE-SET FOLDER	DESCRIPTION
Windows Events	Contains rules tailored for PCI Requirements, Security logs, System Health logs, noise reduction and more.
SQL Server Audits	Contains rules tailored for SQL Server Audit monitoring. Amongst others, these include: <ul style="list-style-type: none">» Database changes» Server changes» Database access.
SNMP Traps	Contains rules tailored for SNMP Traps Messaging. Amongst others, these include: <ul style="list-style-type: none">» Cisco IOS 12.1» Cisco IOS 12.2» Allied Telesis.
Oracle Audits	Contains rules tailored for Oracle Server Audit monitoring. Amongst others, these include: <ul style="list-style-type: none">» Database changes» Server changes» Database access.

RULE-SET FOLDER	DESCRIPTION
Syslog Messages	<p>Contains rules tailored for the processing LINUX and UNIX system logs. Amongst others, these include:</p> <ul style="list-style-type: none"> » Juniper network rules » IBM iSeries rules » LINUX\UNIX host rules.
Text Logs	<p>Contains rules tailored for the processing of web transfer protocols. Amongst others, these include:</p> <ul style="list-style-type: none"> » HTTP rules » FTP rules » SMTP rules.

8.2 Adding a rule-set folder

To create a new rule-set folder:

1. Click **Configuration** tab and select **Event Processing Rules**.
2. From **Common Tasks**, select **Create folder**.
4. Specify a unique name for the new rule-set folder.



To create sub rule-set folders, right-click on the parent folder and select **Create new folder...**

8.2.1 Renaming and deleting folders

To rename or delete existing rule-set folders, right-click on the target rule-set folder and select **Rename** or **Delete** accordingly.

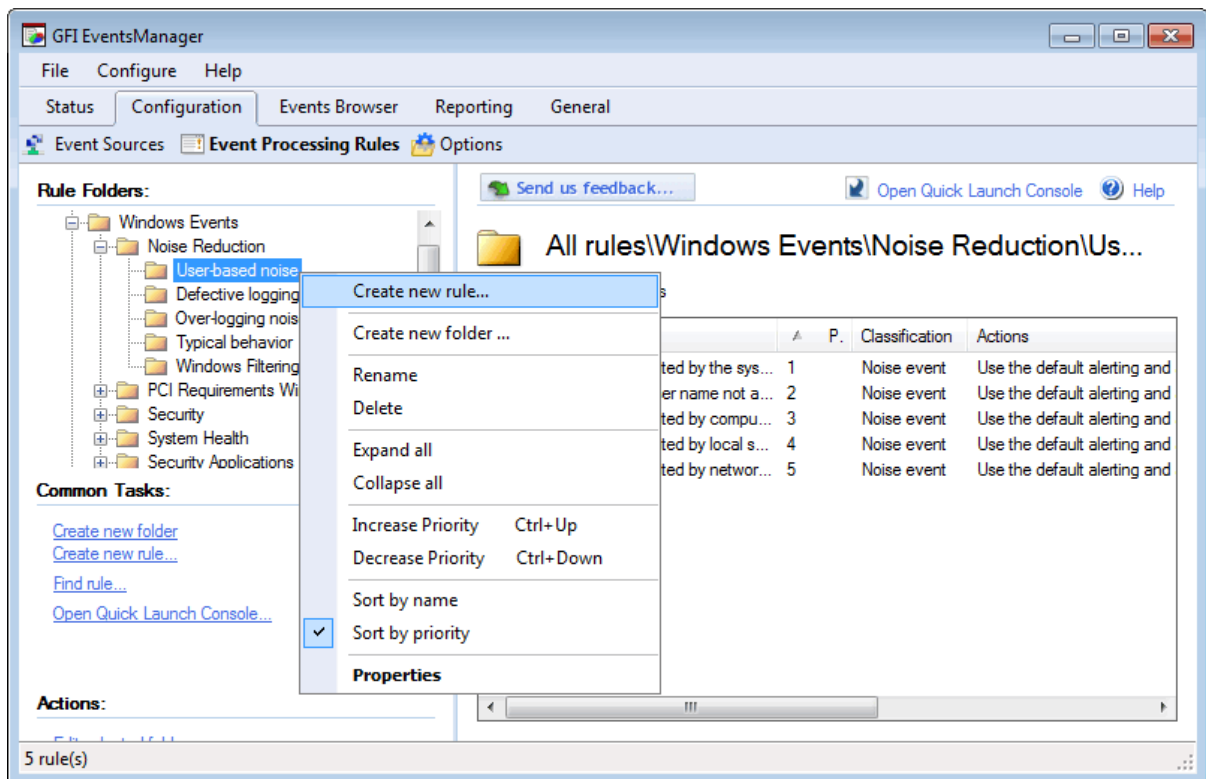


Deleting a rule-set folder will lead to the deletion of all the rules and rule-sets contained within the deleted folder.

8.3 Creating new events processing rules

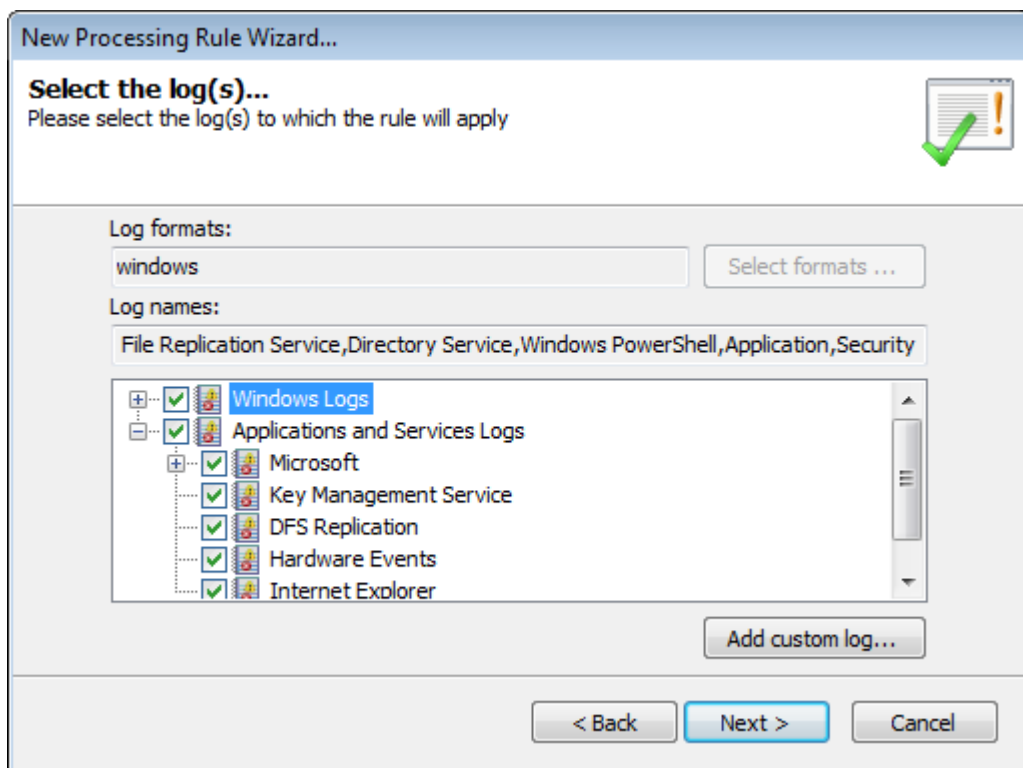
To create a new event processing rule:

1. Click **Configuration** tab and select **Event Processing Rules**.



Screenshot 89 - To create new rules, rich-click a rule-set and select Create new rule...

2. Right-click the rule-set where the new rule will be created and click **Create new rule...**
3. Specify the name and a description (optional) for the new rule. Click **Next**.



Screenshot 90 - Create new events processing rule: Select the logs which the rule will be applied to

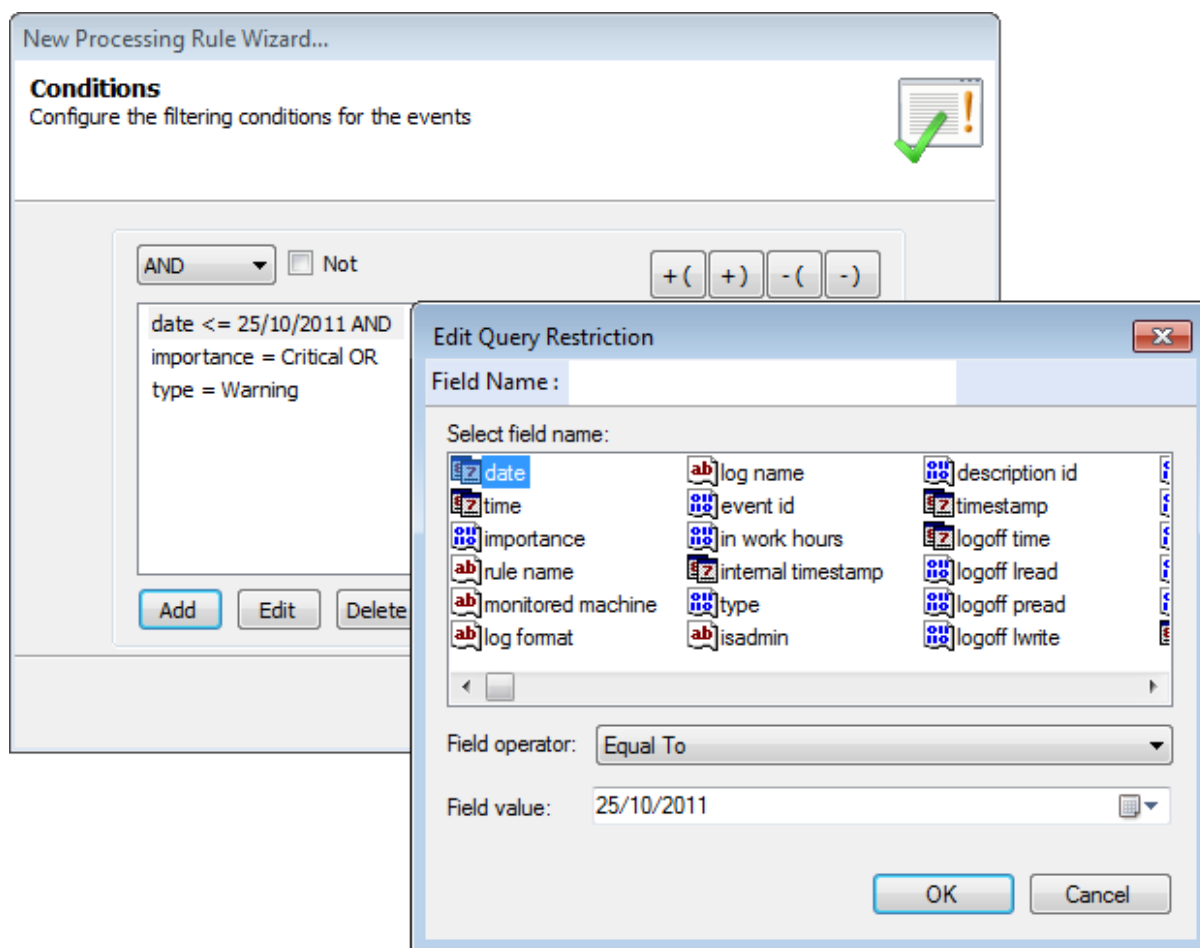
4. Select the event logs to which the rule applies and click **Next**. Optionally, click **Add custom log...** to insert an event log which you preconfigured.



For SQL Audit, Oracle Audit, Syslogs, W3C logs and SNMP Traps messages, specify the full path of the object's log folder; example: "C:\W3C\logs".



For more information, refer to [Collecting Custom Events](#).



Screenshot 91 - Create new events processing rule: Configure the rule conditions

5. Click **Add** to select a field from the list of available fields. Specify the **Field Operator** and **Field Value** and click **OK**. Click **Next**. For more information, refer to [Defining restrictions](#).



Repeat this step until all conditions have been configured.



To create a rule that applies to all events, do not specify conditions.



To filter events that refer to an administrator user (events having the security identifier SID that identifies a logon administrator session), ensure that if the event source is a domain member, the domain controller must also be added as an event source. For more information, refer to [Managing event sources groups](#).

New Processing Rule Wizard...

Select event occurrence and importance
Filter the events on which part of the day the event happen and select their classification level

The rule applies if the event happens:

Classify the event as:

< Back Next > Cancel

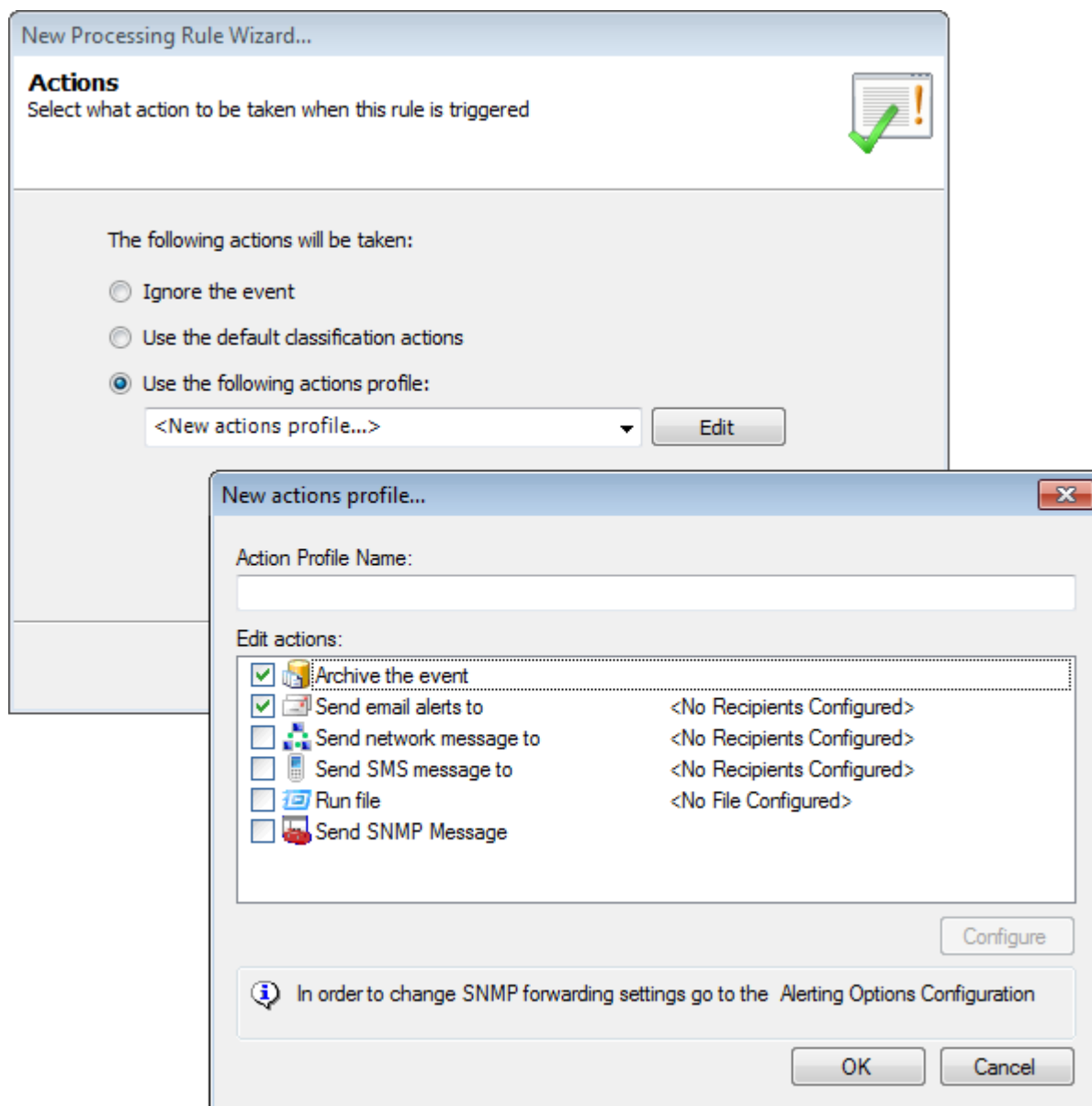
Screenshot 92 - Create new events processing rule: Select the event occurrence and importance

6. Specify the time when the rule is applicable. Example: anytime, during working hours or outside working hours.



Working and non-working hours are based on the operational time parameters configured for your event sources. For more information, refer to [Configure operational time](#).

7. Select the classification (critical, high, medium, low or noise) that will be assigned to events that satisfy the conditions in this rule. Click **Next**.



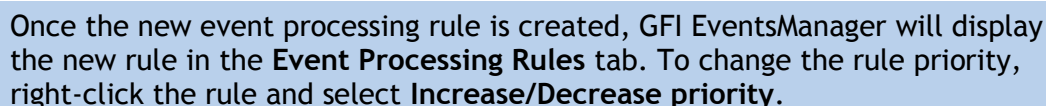
Screenshot 93 - Create new events processing rule: Select the action

8. Specify which actions are triggered by this rule and click **Next**. Available actions are:

Table 59 - Configuring new events processing rules: Actions

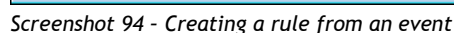
ACTION	DESCRIPTION
Ignore the event	Select this option so that GFI EventsManager will ignore the event and not trigger any actions or notifications.
Use the default classification actions	Select this option to use the preconfigured Default Classification Actions . For more information refer to Configuring Default Classification Actions .
Use the following actions profile	Click Edit and select an action from the New actions profile.... Available actions include: <ul style="list-style-type: none"> » Archive the event » Send email alerts to » Send network message to » Send SMS message to » Run file » Send SNMP Message.

9. Click **Finish** to finalize your settings.



GFI EventsManager enables you to create new rules based on the information of existing events.

1. From **Events Browser**, locate the event log that you want to base the rule upon.



2. Right-click the event and select **Create rule from event**.

Screenshot 95 - New rule from event dialog

3. Configure the options from the tabs described below:

Table 60 - Create rule from event dialog options

TAB	DESCRIPTION
General	Use this tab to configure the general properties of the rule including the rule name and rule classification.
Event Logs	This tab is available only for Windows event logs log rules. Use this tab to specify the Windows event logs for which this rule applies.
Conditions	Use this tab to configure event filtering conditions.
Actions	Use this tab to configure alerts and actions triggered by this rule.
Threshold	Use this tab to configure the event threshold value i.e. the number of times that an event must be detected prior to triggering alerts and remedial actions. This helps reducing false positives triggered by noise (repeated events) in your event logs.

8.5 Advanced event filtering parameters

GFI EventsManager allows systems administrators to set up advanced event filtering parameters. These options are available only for Windows Events and Syslogs.

8.5.1 Windows events conditions

The **Event IDs:** field allows systems administrators to setup parameters described in the table below:

Table 61 - Parameters available in the Event ID field

PARAMETER TYPE	EXAMPLE
Single events	Event IDs: <input type="text" value="575"/>
List of events	Event IDs: <input type="text" value="550, 570"/>

PARAMETER TYPE	EXAMPLE
Range of events	<u>E</u> vent IDs: <input type="text" value="575-600"/>
Combination of events	<u>E</u> vent IDs: <input type="text" value="550, 570, 575-600"/>

The **Source**, **Category** and **User** fields allow systems administrators to setup parameters described in the table below:

Table 62 - Parameters available in the Source, Category and User fields

PARAMETER TYPE	EXAMPLE
Single source name	<u>S</u> ource: <input type="text" value="Userenv"/>
List of sources	<u>S</u> ource: <input type="text" value="Userenv, SceCli"/>
Wildcards (% and *)	<u>S</u> ource: <input type="text" value="S%t%"/>

8.5.2 Syslog categories

The **Message** and **Process** fields allow systems administrators to setup parameters described in the table below:

Table 63 - Parameters available in the Message and Process fields

PARAMETER TYPE	EXAMPLE
Single message	<u>M</u> essage: <input type="text" value="session opened"/>
List of messages	<u>M</u> essage: <input type="text" value="session opened, session closed"/>
Wildcards (% and *)	<u>M</u> essage: <input type="text" value="%session opened%"/>

9 Customizing alerts and actions

9.1 Introduction

This chapter sections that contain information about:

- » [Configuring Default Classification Actions](#)
- » [Configuring Alerting Options](#)

During event processing, GFI EventsManager can automatically generate various actions whenever particular events are encountered. Supported actions include email alerts and event archiving.

You can specify alerts and actions to be triggered in two ways:

Table 64 - Alerting methods

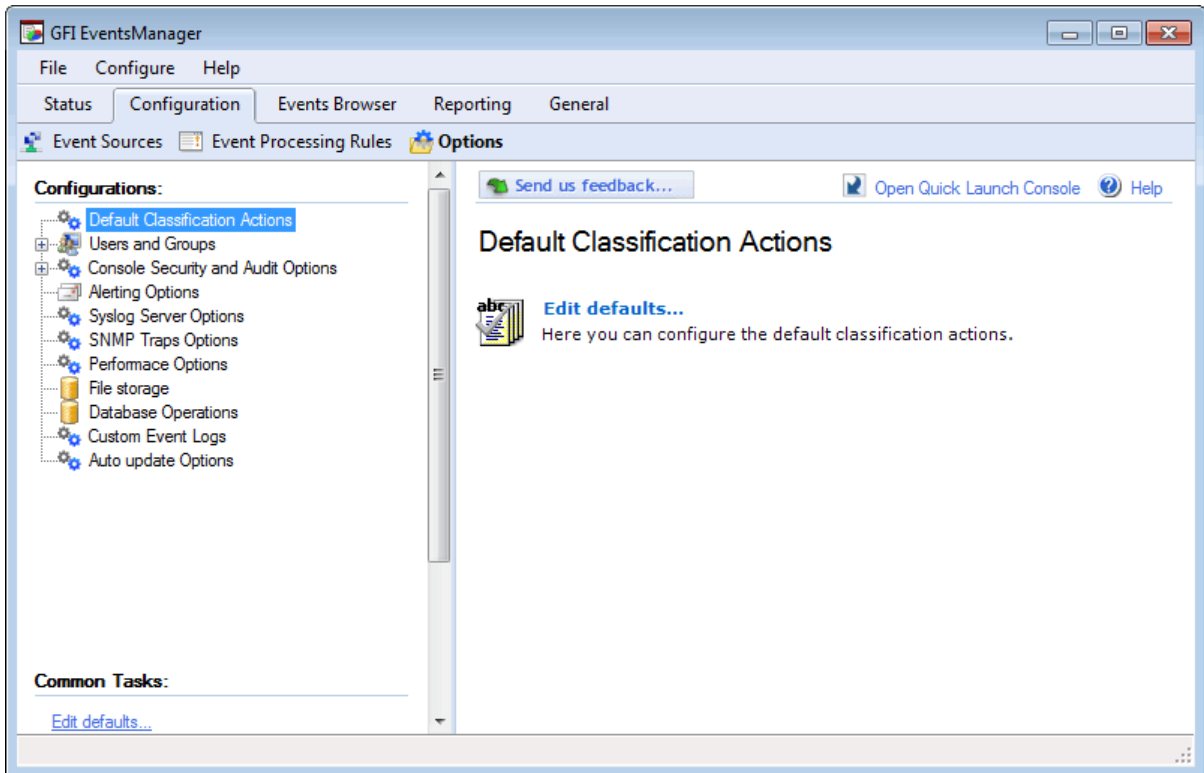
METHOD	DESCRIPTION
Default classification actions	Through the configuration parameters provided in the default classification actions, you can trigger alerts and actions based only on event classification. Example: default classification parameters can be configured to trigger email alerts for all classified events (critical, high, medium and low) but archive only critical events.
Creating or customizing rules and rule-sets	Rules allow you to configure actions on a more granular level. Rules allow you to configure and trigger actions whenever an event fits one or more specific conditions. Example: you can create a rule which archives only events having event ID 231, regardless their classification.

GFI EventsManager supports the following actions:

Table 65 - Supported alerting actions

ACTION	DESCRIPTION
Archive the event	Archives the classified event into the GFI EventsManager database back-end.
Send e-mail, SMS, network or SNMP notifications to	Sends email, SMS network or SNMP alerts to specific recipients.
Run File	Runs an executable file. Files that can be executed include VBScripts (.VBS), Batch files (.BAT) or another executable type of file (.EXE). You can also specify any command-line parameters to pass on to the executable file.

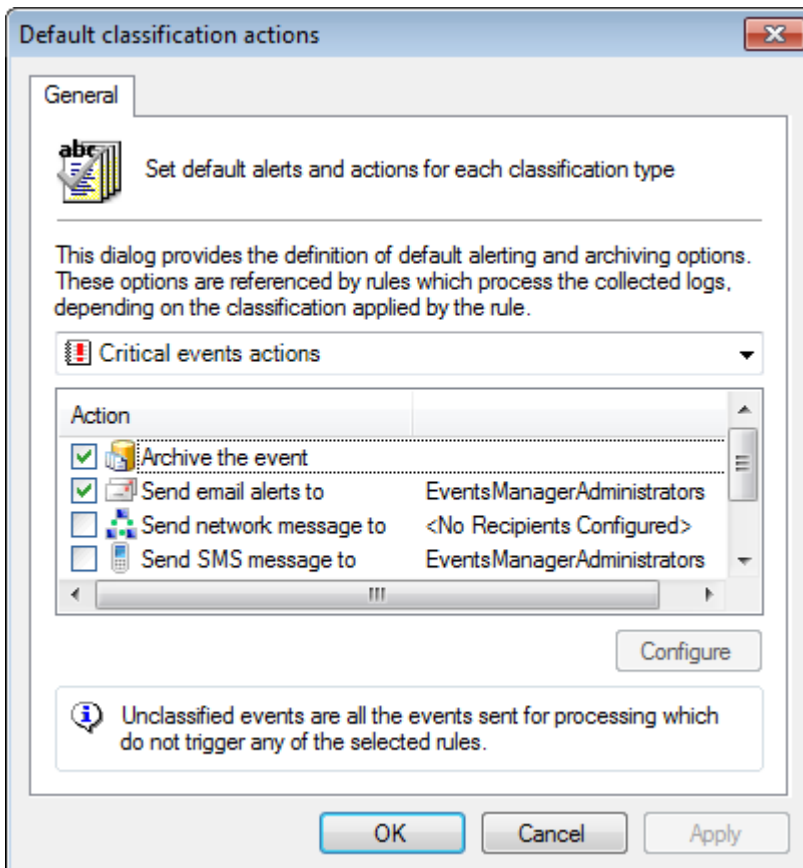
9.2 Configuring Default Classification Actions



Screenshot 96 - Configuring default classification actions

To configure default classification actions:

1. Click the **Configuration** tab and select **Options**.
2. From Configurations, right-click on the **Default Classification Actions** node and select **Edit defaults....**



Screenshot 97 - Default Classification Actions dialog

3. From the drop-down menu, select the event classification to be configured.
4. From **Action** list, select actions to be triggered for the selected classification.
5. Click **Configure** to specify any parameters required by the selected action.
6. Click **OK** to finalize your settings.

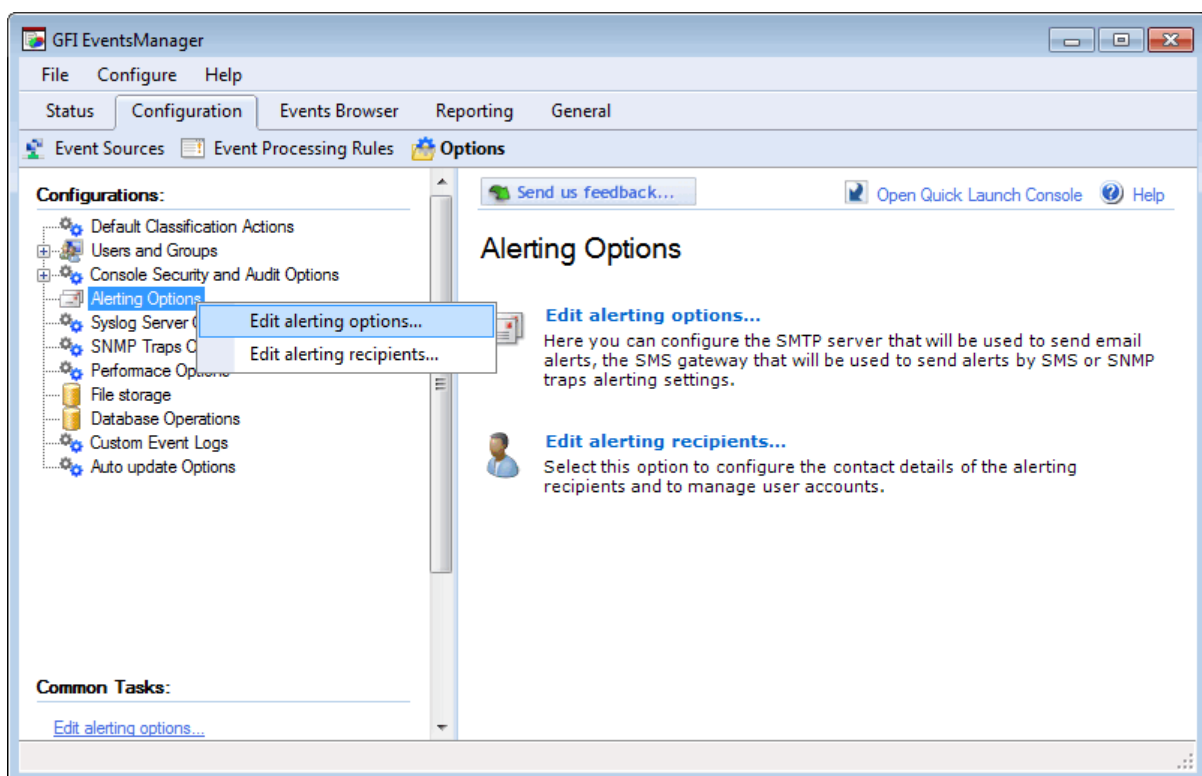


Running default actions on events classified as Low events actions may cause a lot of network traffic when email, SMS, network or SNMP alerts are enabled. This may also be problematic when archiving is enabled on Low importance events.

9.3 Configuring Alerting Options

Alerting options enable you to configure what alerts are triggered when particular event(s) are captured. For example, you can configure GFI EventsManager to send an email and SMS alert to one or more recipients when a Critical event is processed.

To configure Alerting Options:



Screenshot 98 - Configuring Alerting Options

1. Click **Configuration** tab and select **Options**.
2. From **Configurations**, right-click on the **Alerting Options** node and select **Edit alerting options...** option.



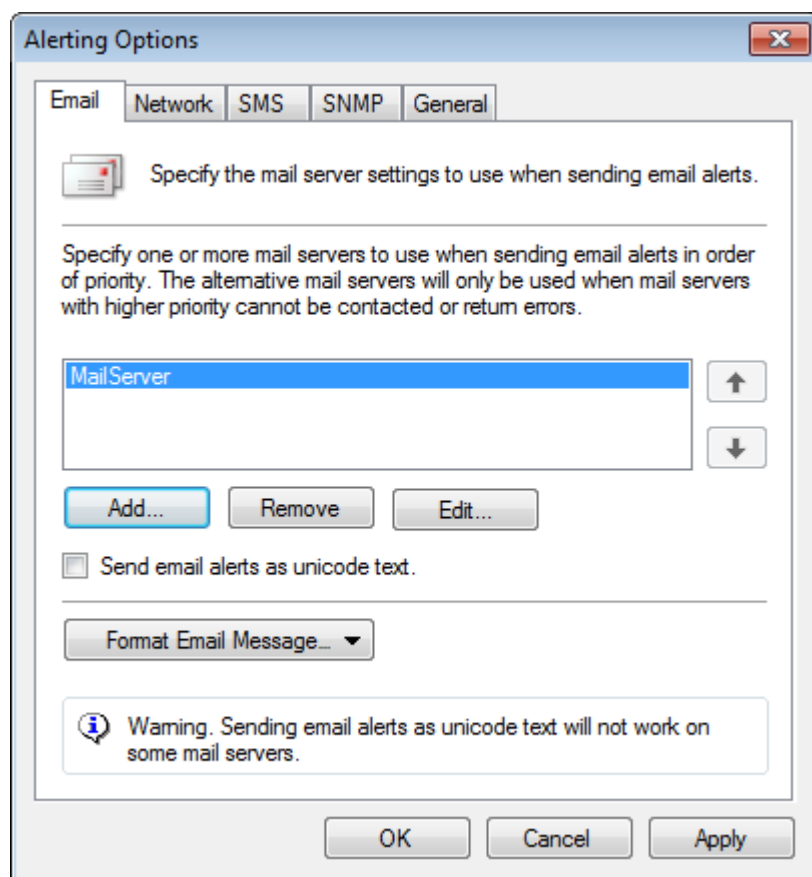
Select **Edit alert recipients** to configure the contact details of the alerting recipients and to manage user accounts. For more information, refer to [Managing user accounts](#).

3. Configure the alerting method of your choice. The following sections describe how alerting is configured:

- » [Configuring email alerts](#)
- » [Configuring network alerts](#)
- » [Configuring SMS alerts](#)
- » [Configuring SNMP alerts](#)
- » [Configuring General alerts](#)

9.3.1 Configuring email alerts

To configure email alerts:



Screenshot 99 - Configuring Email options

1. From the **Alerting Options** dialog, click **Email** tab.
2. Configure the options described below:

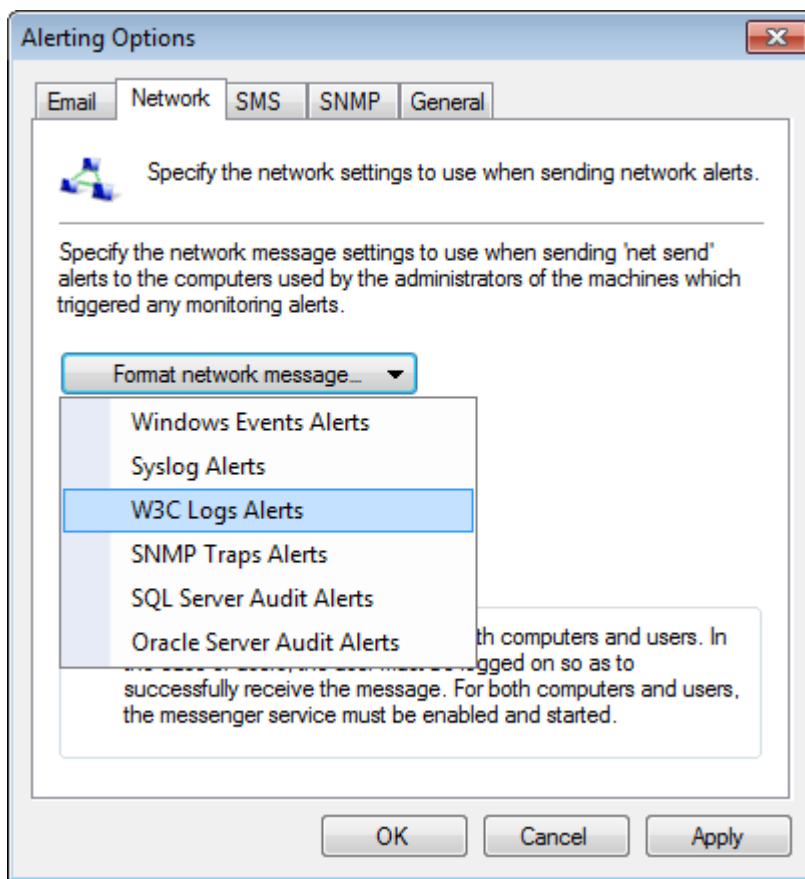
Table 66 - Alerting Options dialog: Email

OPTION	DESCRIPTION
Add/Remove/Edit	Click Add... to specify the mail server details including the server name /IP, logon credentials and recipient email address. Use the Remove or Edit button to remove a selected server or edit details.
Up/Down arrow buttons	Use the arrow buttons to change the position of the selected mail server. GFI EventsManager attempts to deliver email alerts via the first mail server. If unsuccessful, it recursively checks the following mail servers.
Send email alerts as Unicode text	Select this option to send emails as Unicode text as opposed to HTML or RTF format.
Format Email Message	Optionally, from the Format Email Message drop-down menu, select the log type (Windows, W3C, Syslog) and customize the email content.

3. Click **OK** to finalize your settings.

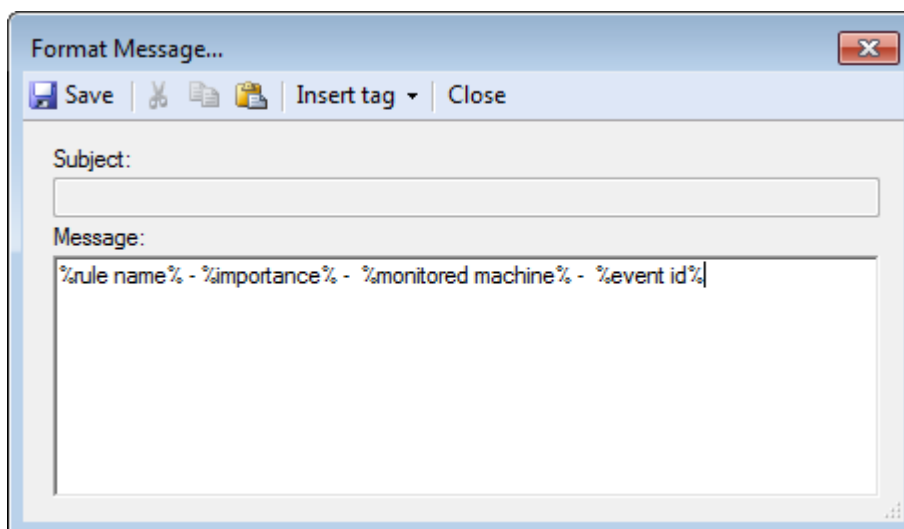
9.3.2 Configuring network alerts

To configure network alerts:



Screenshot 100 - Configuring Network alerts

1. From the **Alerting Options** dialog, click **Network** tab.
2. From **Format network message...** drop-down menu, select the log type and customize the format of the message.

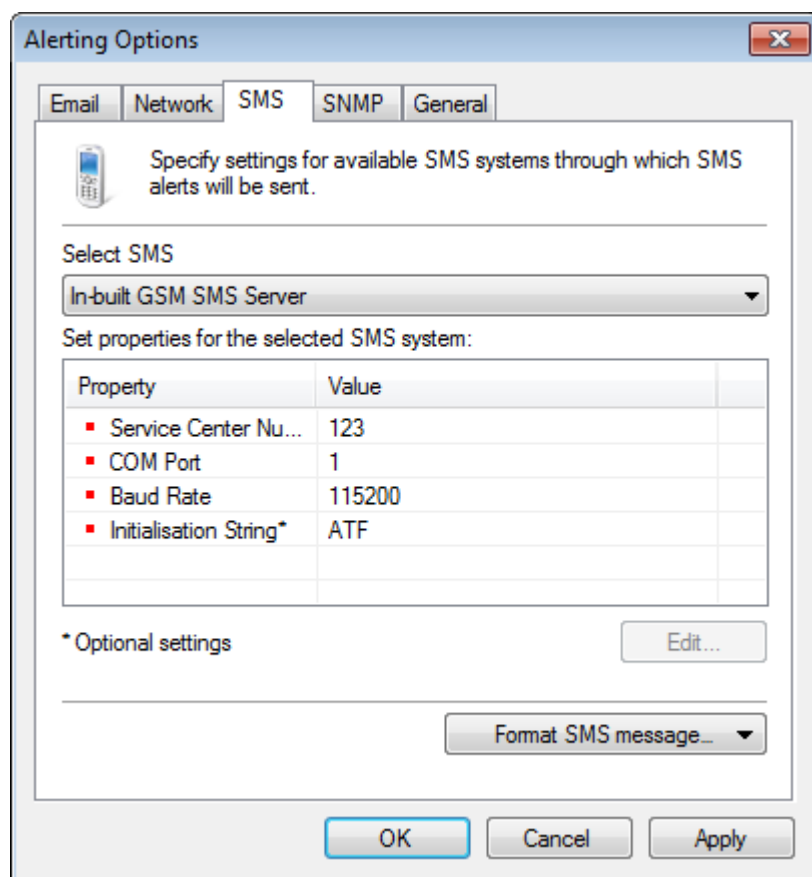


Screenshot 101 - Configuring Network alerts: Format message dialog

3. Click **Insert tag** to select from a list of tags to include in the message.
4. Click **Save** and **OK** to finalize your settings.

9.3.3 Configuring SMS alerts

To configure SMS alerts:



Screenshot 102 - Configuring SMS alerts

1. From the **Alerting Options** dialog, click **SMS** tab.
2. Configure the options described below:

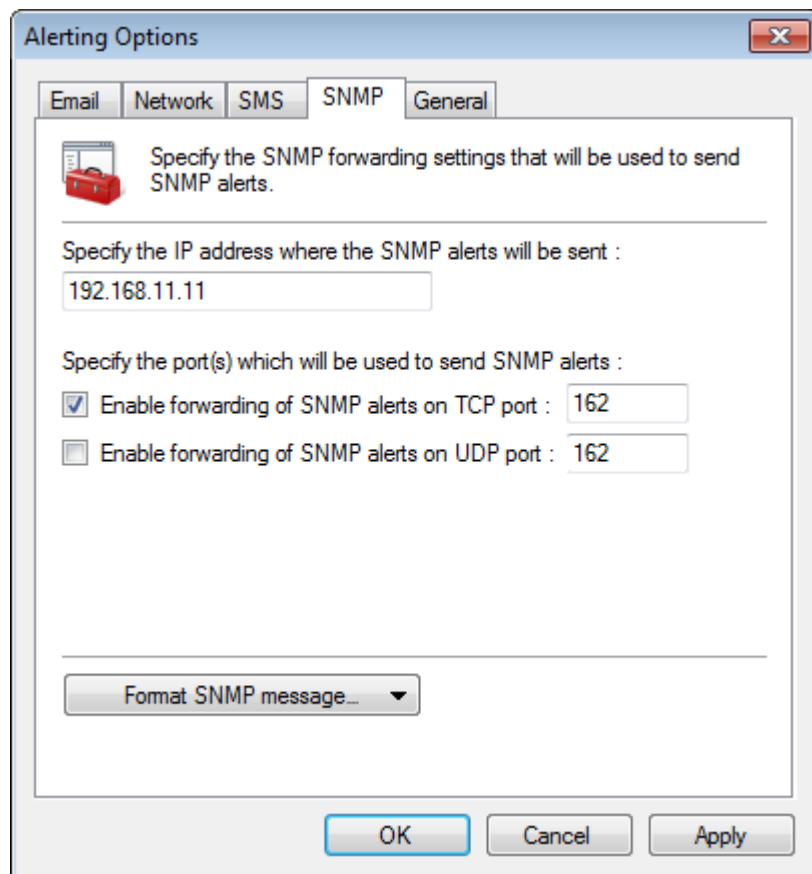
Table 67 - Alerting Options dialog: SMS

OPTION	DESCRIPTION
Select SMS	Select the SMS service used to send SMS alerts. Available services include: <ul style="list-style-type: none">» In-built GSM SMS Server» FaxMaker SMS service provider template» Clickatell Email2SMS Service» Generic SMS service provider template.
Set properties for the selected SMS system	Configure the properties for the selected SMS service type. Amongst others, property settings include: <ul style="list-style-type: none">» Service center number» COM Port» Baud Rate» SMTP Server» SMTP Port. Click Edit... to configure the selected property.
Format SMS message	Optionally, from the Format Email Message drop-down menu, select the log type (Windows, W3C, Syslog) and customize the email content.

3. Click **OK** to finalize your settings.

9.3.4 Configuring SNMP alerts

To configure SNMP alerts:



Screenshot 103 - Configuring SNMP alerts

1. From the **Alerting Options** dialog, click **SNMP** tab.
2. Configure the options described below:

Table 68 - Alerting Options dialog: SNMP

OPTION	DESCRIPTION
Specify the IP address where the SNMP alerts will be sent	Enter the IP address of the recipient.
Specify the port(s) which will be used to send SNMP alerts	Specify TCP/UDP communication port. By default, the assigned port is 162.
Format SNMP message	Optionally, from the Format Email Message drop-down menu, select the log type (Windows, W3C, Syslog) and customize the email content.

3. Click **OK** to finalize your settings.

9.3.5 Configuring General alerts

To configure database status alerts:

1. From the **Alerting Options** dialog, click **General** tab.
2. Configure the options described below:

Table 69 - Alerting Options dialog: General

OPTION	DESCRIPTION
Send email alerts on database errors	Email alerts are sent upon database errors such as backup failure, data corruption, size exceeds maximum size specified and other database operation errors.

OPTION	DESCRIPTION
Send email alerts on completion of database rollover	Email alerts are sent when a database rollover is complete.

3. Click **OK** to finalize settings.

10 Configuring users and groups

10.1 Introduction

Use the Users and Groups node to assign different console access privileges to GFI EventsManager users. Through this node users and groups can be configured, amended or deleted. Working hours and alerts can also be configured and assigned to groups. Refer to the following sections for more information:

- » [Managing user accounts](#)
- » [Managing groups](#)
- » [Managing console security and audit options](#)
- » [Managing Database and Files Backend security](#)

10.2 Managing user accounts

This section contains information about:

- » [Configuring the administrator account](#)
- » [Creating a new user](#)
- » [Changing user properties](#)
- » [Deleting users](#)

10.2.1 Configuring the administrator account

GFI EventsManager will automatically create an **EventsManagerAdministrator** account. However, you must still configure details such as the email address and mobile number of the GFI EventsManager administrator.



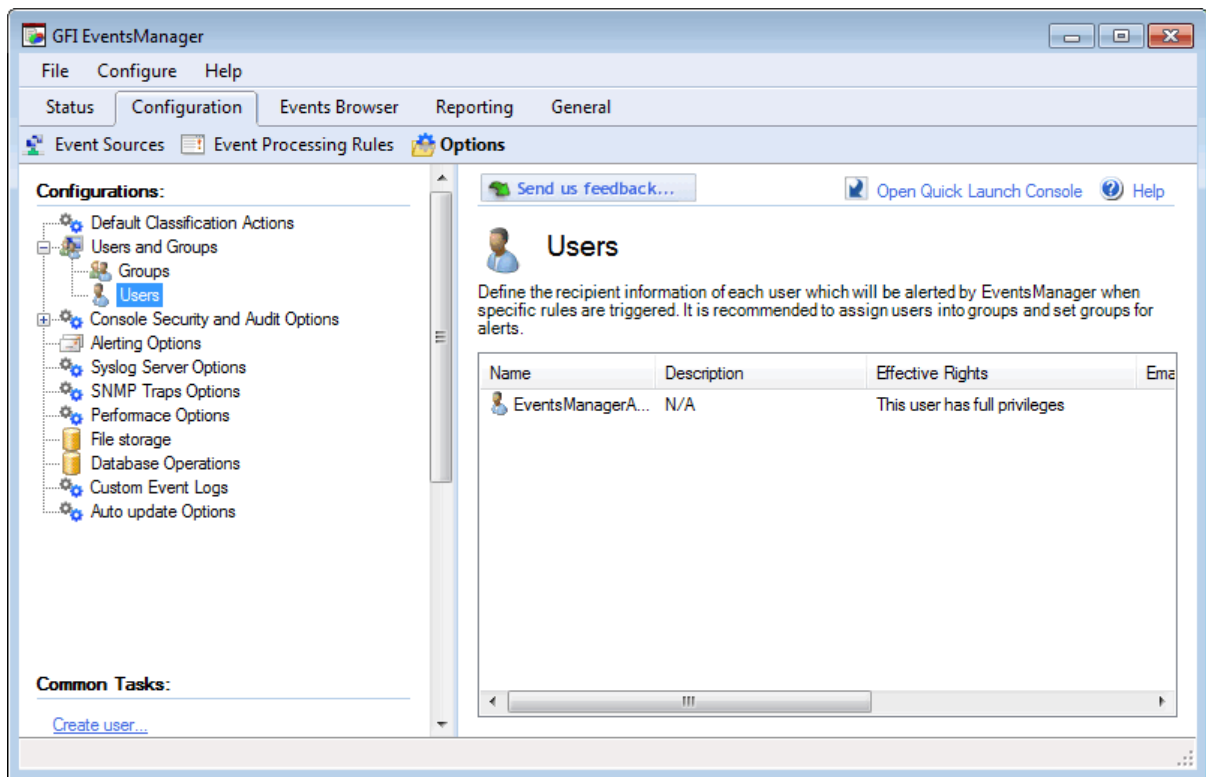
GFI EventsManager requires a valid administrator email address in order to distribute automatic alerts when particular events are discovered.

For every user (including the administrator), you can configure the following parameters:

- » Contact details including email address and phone number
- » The typical working hours
- » The type of alert to send during and outside working hours
- » The notification group to which the user belongs.

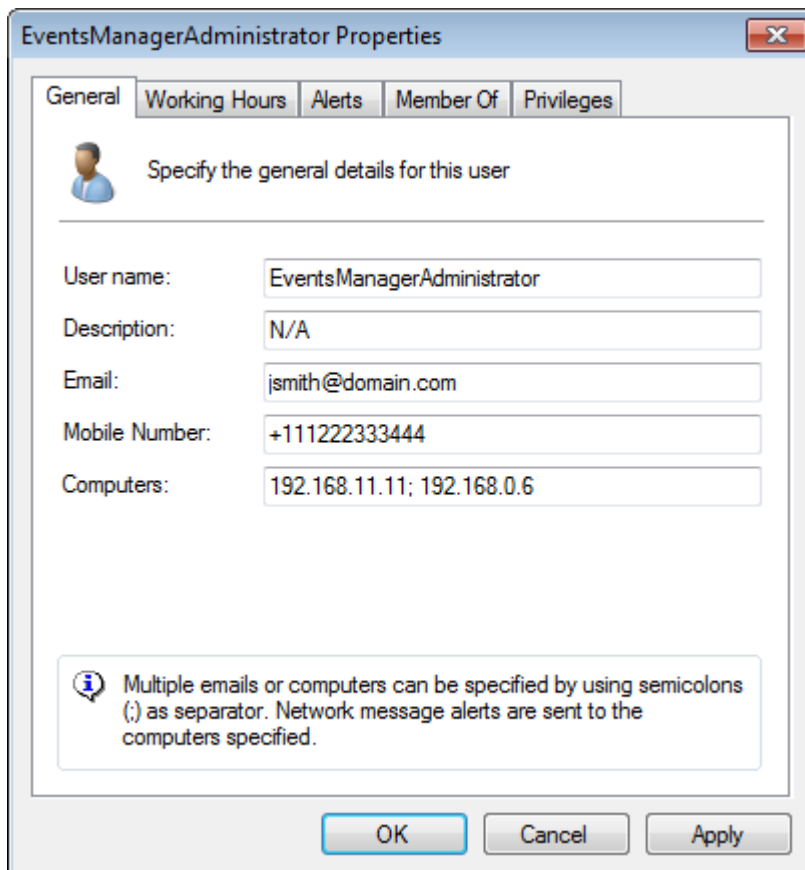
To configure the GFI EventsManagerAdministrator account:

1. Click **Configuration** tab and select **Options**.



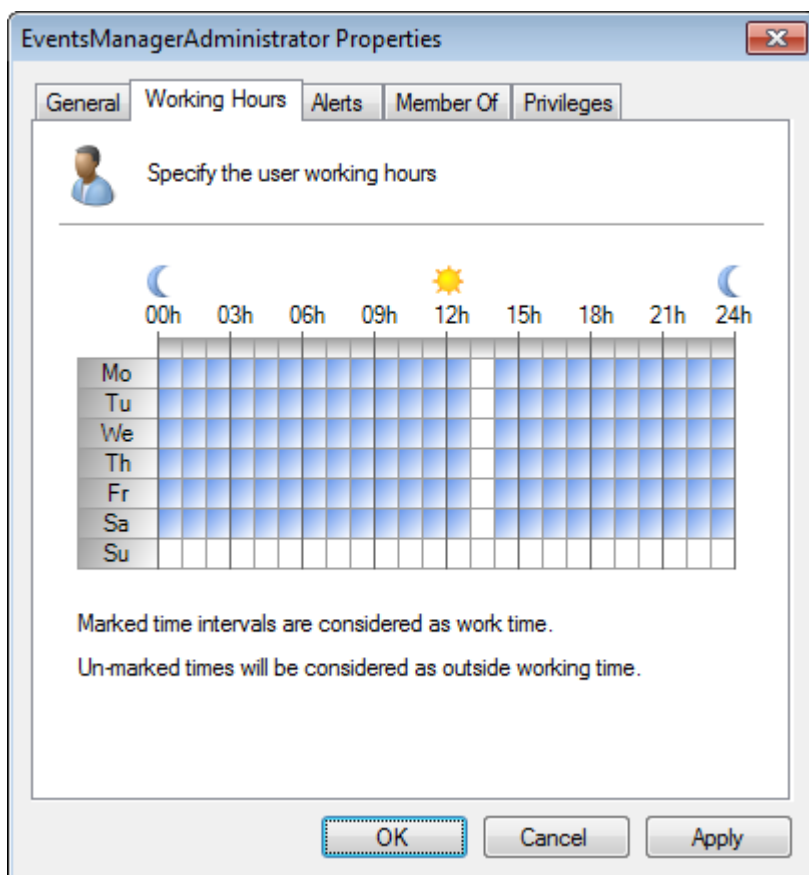
Screenshot 104 - Configuring User settings

2. Expand the **Users and Groups** node and select **User** sub-node.
3. From the right pane, right-click **EventsManagerAdministrator** and click **Properties**.



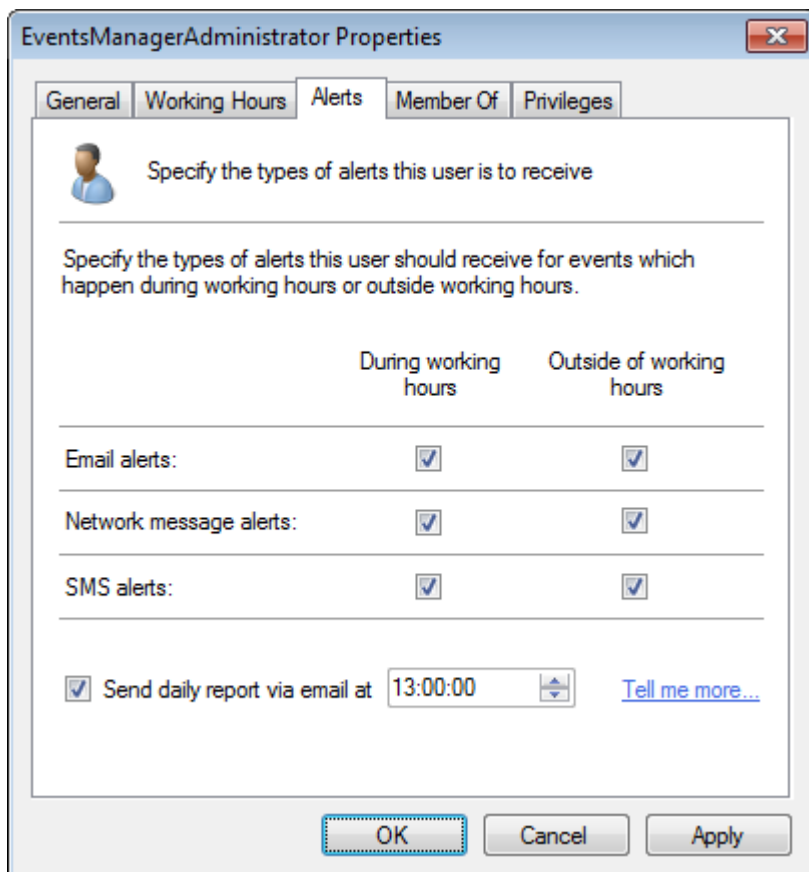
Screenshot 105 - EventsManager Administrator properties

4. Specify the contact details such as email address, and mobile number as required.
5. Specify the computers on which network alerts addressed to the administrator will be sent.



Screenshot 106 - Configuring the typical working hours of an alert recipient

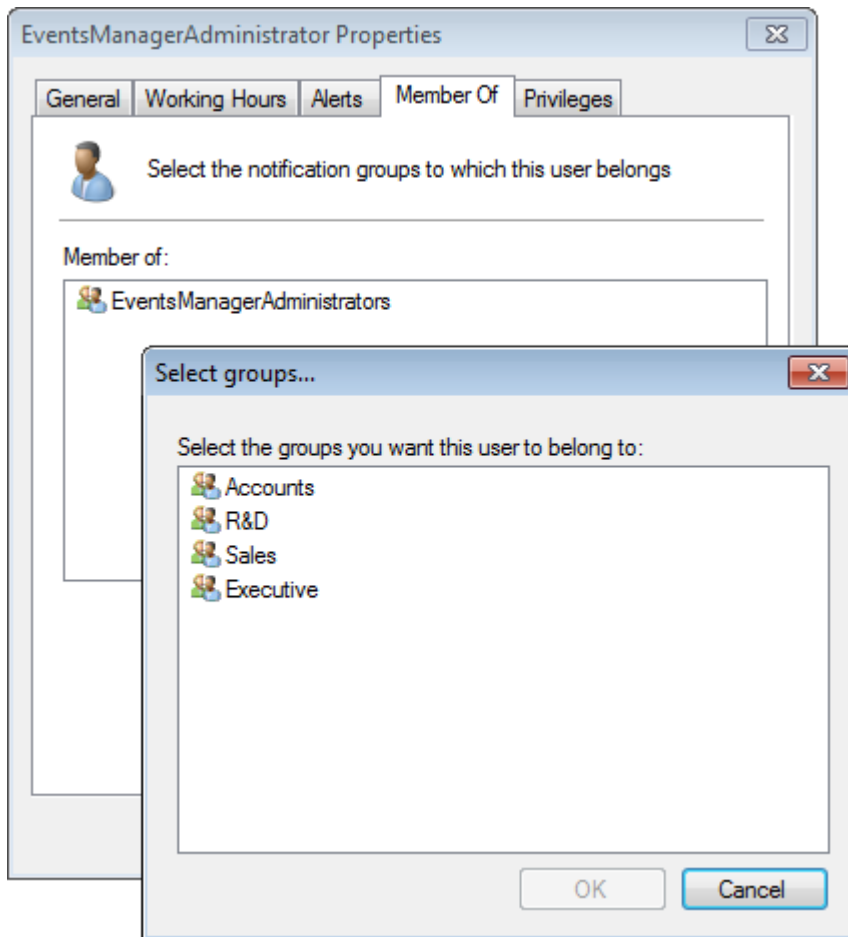
6. Click **Working Hours** tab and specify the typical working hours of the administrator.



Screenshot 107 - Selecting alerts to be sent during and outside working hours

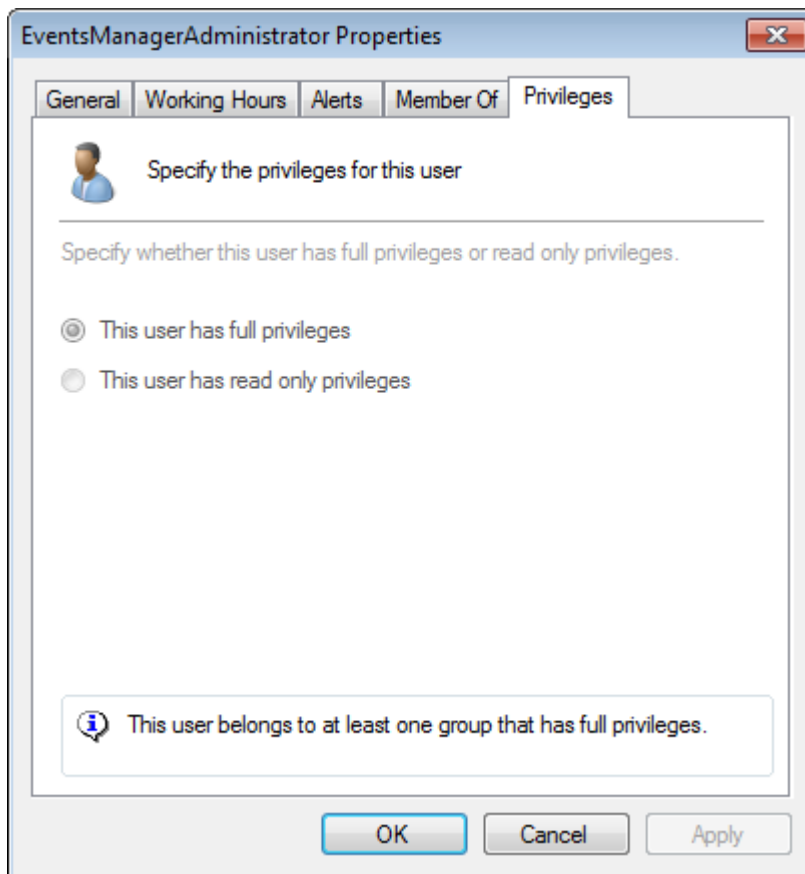
5. Click **Alerts** tab and select which alerts will be sent during and outside working hours.

6. (Optional) Select **Send daily report via email** to send a summary of the most important events collected and processed by GFI EventsManager by email.



Screenshot 108 - Notification groups to which a user belongs

7. Click **Member Of** tab and select the notification groups to which the user belongs. By default the administrator is a member of the **EventsManagerAdministrators** notification group.



Screenshot 109 - Configuring GFI EventsManager administrator privileges

8. Click **Privileges** to modify the user privileges. By default the **EventsManagerAdministrator** account has full privileges.

9. Click **OK** to finalize your settings.

10.2.2 Creating a new user

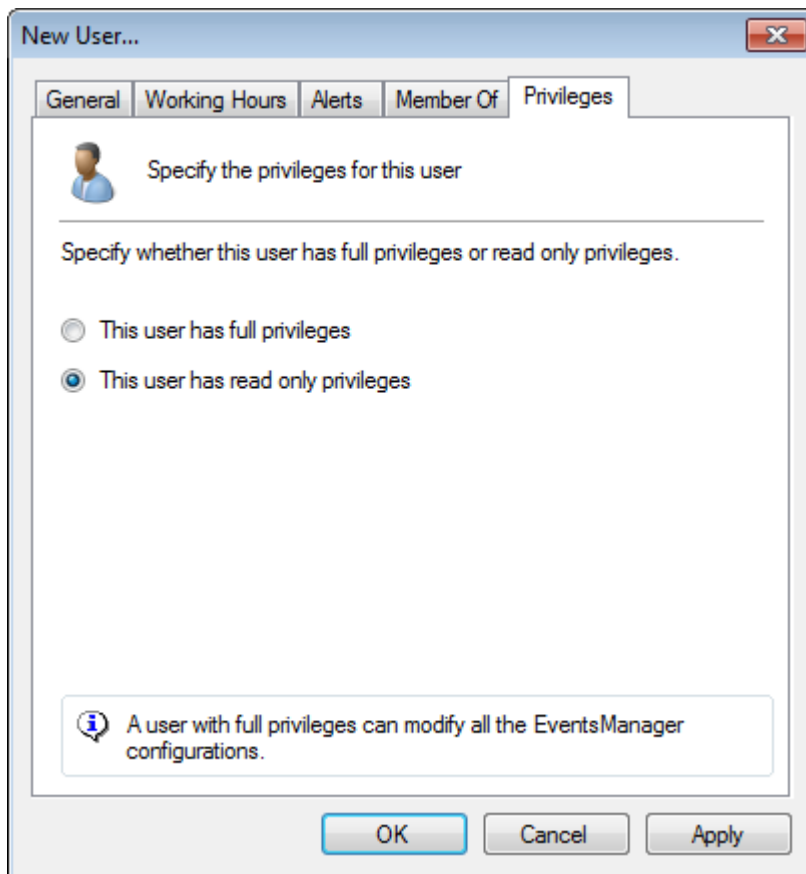
GFI EventsManager allows you to create a custom list of users which you can organize into groups to speed up administrative tasks.

To create a new user:

1. Click **Configuration** tab and select **Options**.
2. Expand the **Users and Groups** node.
3. Right-click on the **Users** sub-node and select **Create user...**
4. Specify the parameters requested in the **General**, **Working Hours**, **Alerts**, and **Member of** tabs.



For more information, refer to [Configuring the administrator account](#).



Screenshot 110 - GFI EventsManager new user privileges

5. Click **Privileges** tab and select user privileges accordingly. Example, to assign administrative privileges to a user select the **This user has full privileges** option.



Users with administrative privileges can modify all GFI EventsManager configuration settings.

6. Click **OK** to finalize setup.

10.2.3 Changing user properties

To edit user properties:

1. From the left pane, click on the **Users** node.
2. Right-click on the user to edit and select **Properties**.
3. Make the required changes in the tabs available and click **OK** to finalize your settings.

10.2.4 Deleting users

To delete a user:

1. From the left pane, click on the **Users** node.
2. From the right viewer pane, right-click on the user to be deleted and select **Delete**.

10.3 Managing groups

GFI EventsManager enables you to assign users to a group. Once the group properties have been configured, every member of the group inherits the same settings. This section contains information about:

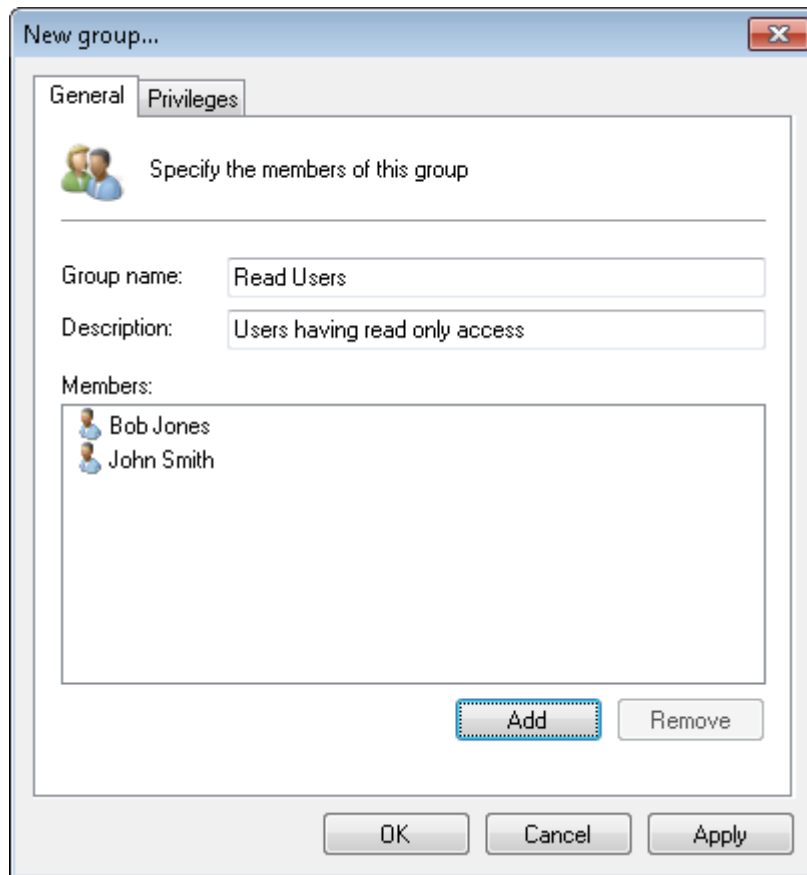
- » [Creating a group](#)
- » [Changing user group properties](#)

» Deleting user groups

10.3.1 Creating a group

To create a group:

1. Click **Configuration** tab and select **Options**.
2. Expand the **Users and Groups** node.
3. Right-click **Groups** sub-node and select **Create group...**



Screenshot 111 - New groups setup

4. Specify the name and an optional description for the new group.
5. Click **Add** to start adding users to the group.
6. From the **Privileges** tab, select if the group has **Full** or **Read Only** permissions.
6. Click **OK** to finalize settings.

10.3.2 Changing user group properties

To edit the settings of a user group:

1. From Configuration tab ► Configurations, expand the Users and Groups node.
2. Right-click on the group to be configured and select **Properties**.
3. Perform the required changes in the tabs available and click **OK** to finalize settings.

10.3.3 Deleting user groups

To delete a user group:

1. From the left pane, click **Groups** node.
2. From the right viewer pane, right-click on the group to be deleted and select **Delete**.

10.4 Managing Console Security and Audit Options

This section contains information about:

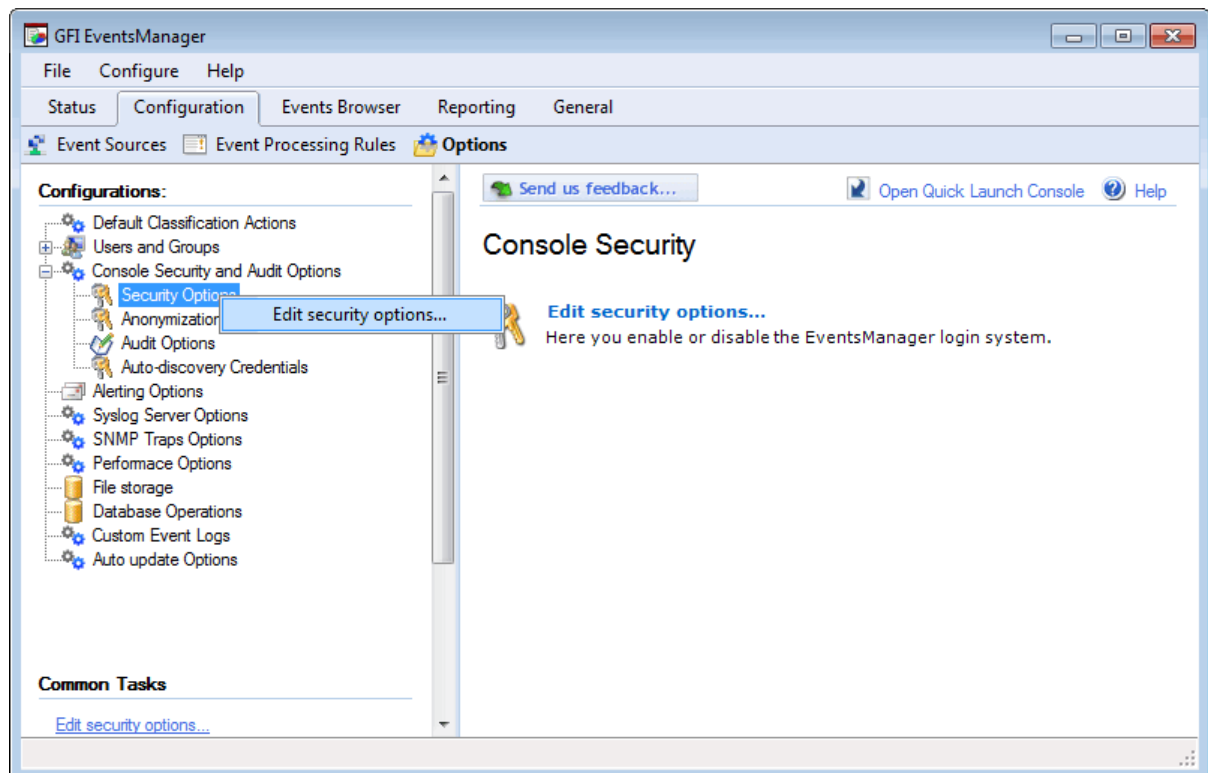
- » [GFI EventsManager login system](#)
- » [Password recovery](#)
- » [Anonymization](#)
- » [Audit console activity](#)
- » [Auto-discovery credentials](#)

10.4.1 GFI EventsManager login system

The Security Options node enables you to configure the GFI EventsManager login system.

To enable the log-in system:

1. Click **Configuration** tab and select **Options**.



Screenshot 112 - Select Security Options to enable the log-in system

2. Expand Console Security and Audit Options node, right-click Security Options node and select Edit security options....
3. Select Enable EventsManager login system to enable login.
4. Click **OK** to finalize settings.



The User must have a valid email address configured in GFI EventsManager to receive the password by email. For more information on how to change user settings including the email address, refer to [Changing user properties](#) in this chapter.



When the login system is enabled all users will be asked to specify their credentials every time they launch the GFI EventsManager management console.



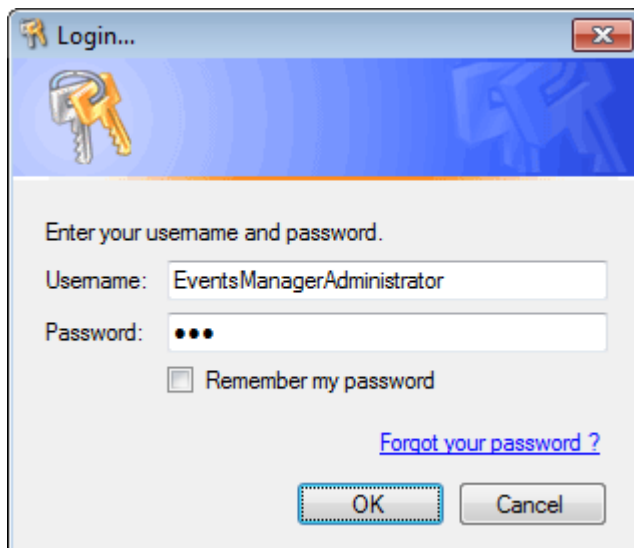
Users are granted access with administrative or user privileges according to the user privileges set up in the privileges tab within the user setup dialogs.



To configure or edit a user password, from **Configuration** tab ► **Users and Groups** ► **Users**, right-click the user account and select **Change Password**.

10.4.2 Password recovery

When GFI EventsManager login system is enabled, all users are requested to enter a valid user name and password to access GFI EventsManager console.



Screenshot 113 - Login window

If a password is forgotten or lost:

1. Key in your username.
2. Click **Forgot your password? Link**

GFI EventsManager will send an email containing your login password.

10.4.3 Anonymization

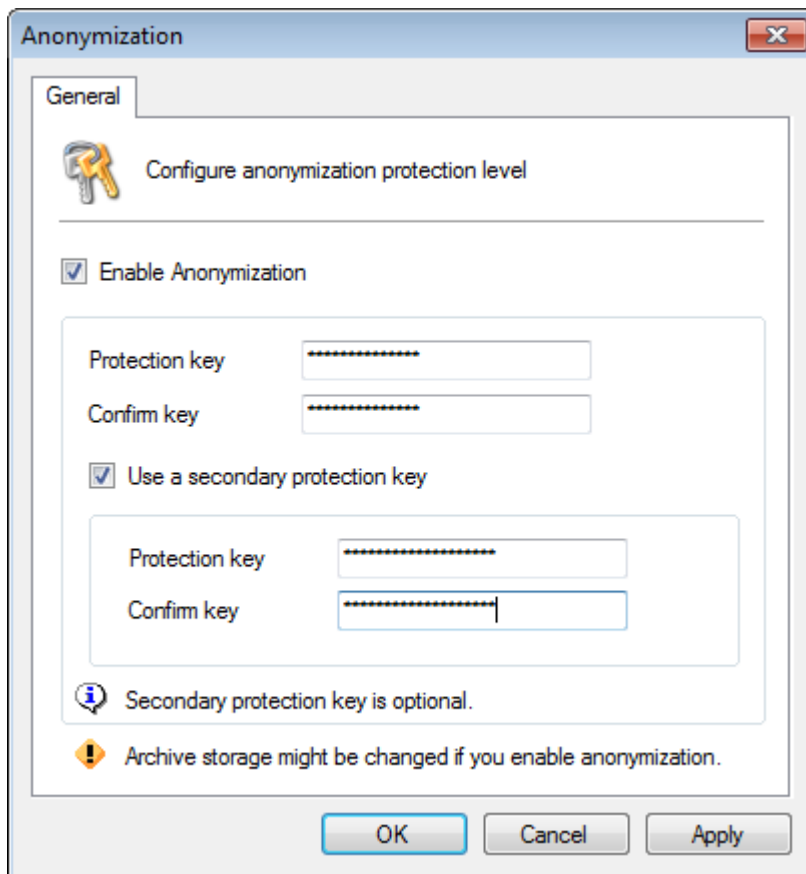
In some countries privacy laws state that it is against the law not to encrypt personal information retrieved by monitoring applications for privacy protection.

GFI EventsManager enables you to encrypt personal information when exporting and/or viewing event logs.

Enable anonymization to encrypt all personal information. The Events Browser and Dashboard can recognize such information and do not display it. Instead, they display **<encrypted>** or **Anonymized data** messages.

To configure anonymization:

1. From **Configuration** tab click **Options**.
2. Expand **Console Security and Audit Options** node, right-click **Anonymization** and click **Edit anonymization options...**



Screenshot 114 - Anonymization options

3. Select **Enable Anonymization** and enter the encryption password.
4. (Optional) Select **Use a secondary protection key** to use two passwords for event log encryption. Event logs can only be decrypted by providing two decryption passwords.
5. Click **OK** to finalize settings.

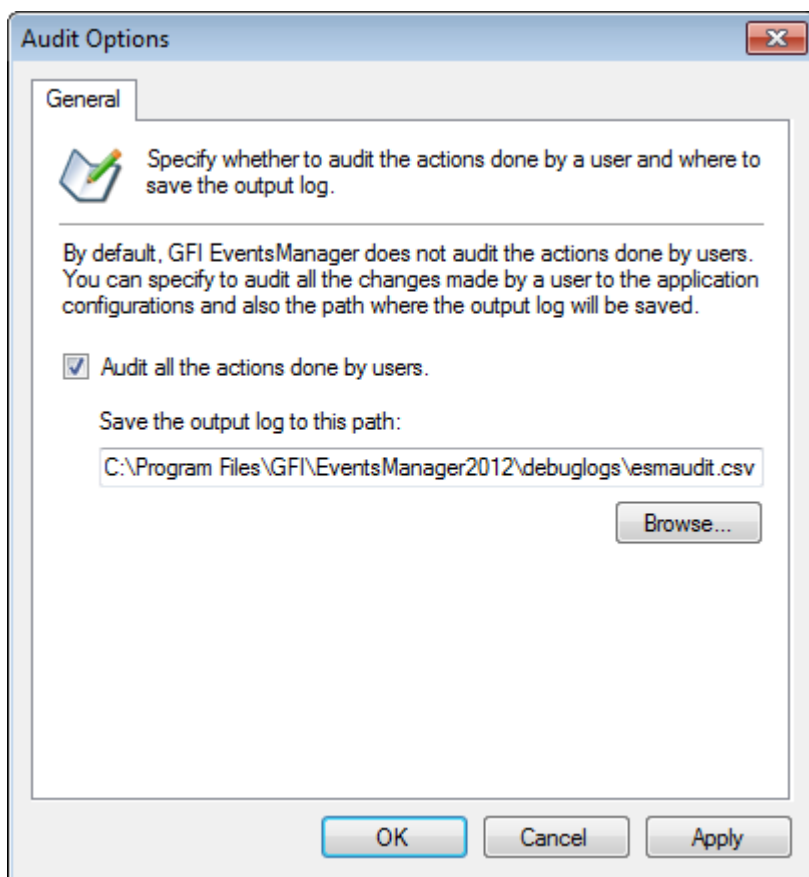


When anonymization is enabled, events that are stored into the central database are encrypted. For information, refer to [Create new anonymization job](#).

10.4.4 Audit console activity

GFI EventsManager can save the console activity to external logs. To configure the console activity auditing:

1. Click **Configuration** tab and select **Options**.
2. Expand Console Security and Audit Options node, click Audit Options node and select Edit audit options....



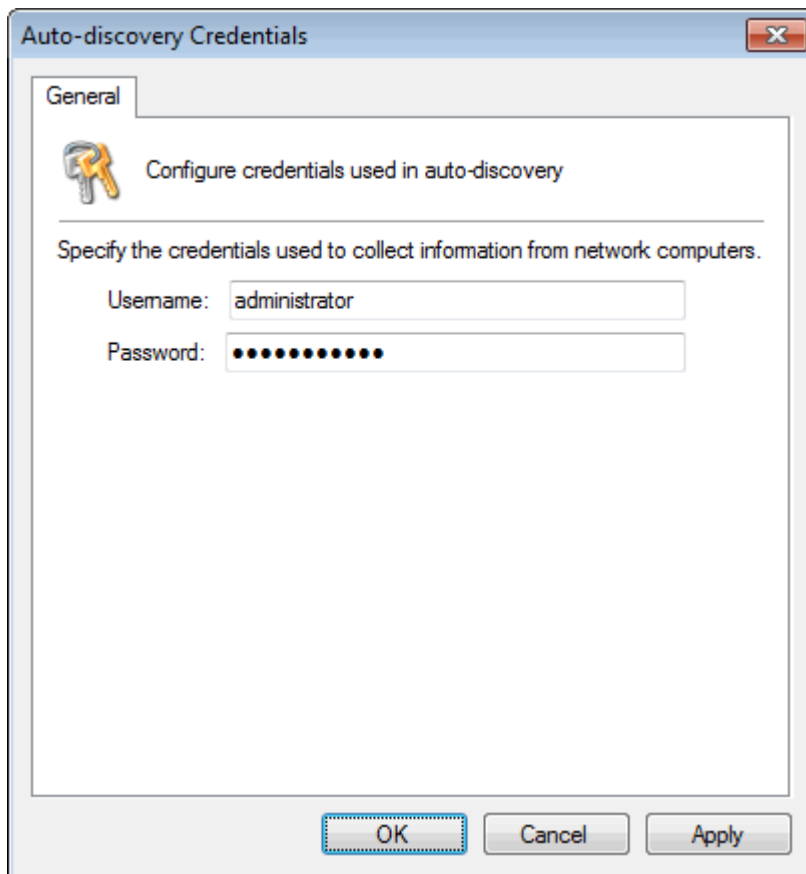
Screenshot 115 - Audit Options

3. Select **Audit all the actions done by users** option and specify the location where the output log file will be saved.
4. Click **OK** to finalize settings.

10.4.5 Auto-discovery credentials

The Auto-discovery credentials are used by GFI EventsManager to login target machines and collect information when performing an automatic search for event sources. To configure the auto-discovery credentials:

1. Click **Configuration** tab ► **Options**.
2. From **Configurations** ► **Console Security and Audit Options**, right-click **Auto-discovery credentials** and select **Edit auto-discovery credentials**.



Screenshot 116 - Auto-discovery credentials

2. Key in a valid username and password. Click **OK**.

10.5 Managing Database and Files Backend security

GFI EventsManager enables you protect your database with an encryption key. Encrypting the database will prevent unauthorized personnel from viewing or accessing event logs.



Encrypting the database will cause the Status Monitor and Events Browser to stop viewing sensitive information.

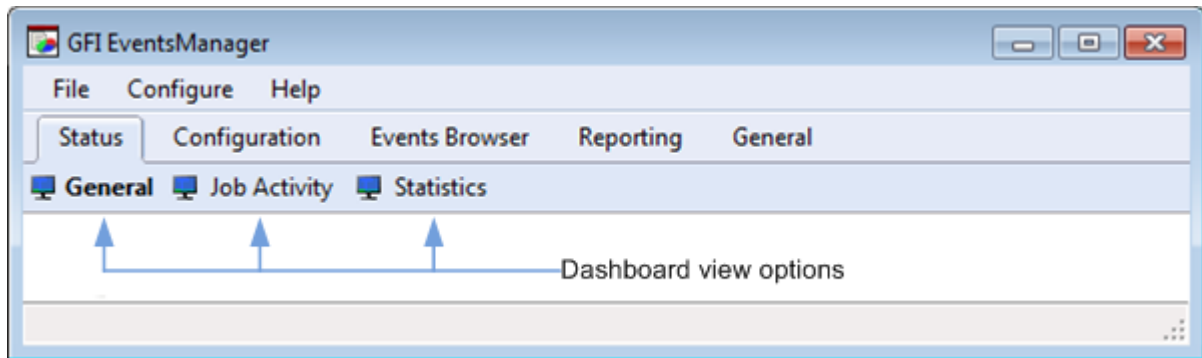
To encrypt the backend database:

1. Click **Configuration** tab ► **Options**.
2. From **Configurations**, click **Database and Files Backend** ► **Configure file storage...**
3. From the **Archive storage** folder dialog, select **Encrypt data using the following password**.
4. Specify the password and click **OK** to save your settings.

11 Status monitoring

11.1 Introduction

The **Status** tab is a dashboard that shows the status of GFI EventsManager as well as statistical information related to the events collected, processed and archived. The status monitor consists of three different dashboard views: **General** view, **Job Activity** view and **Statistics** view.

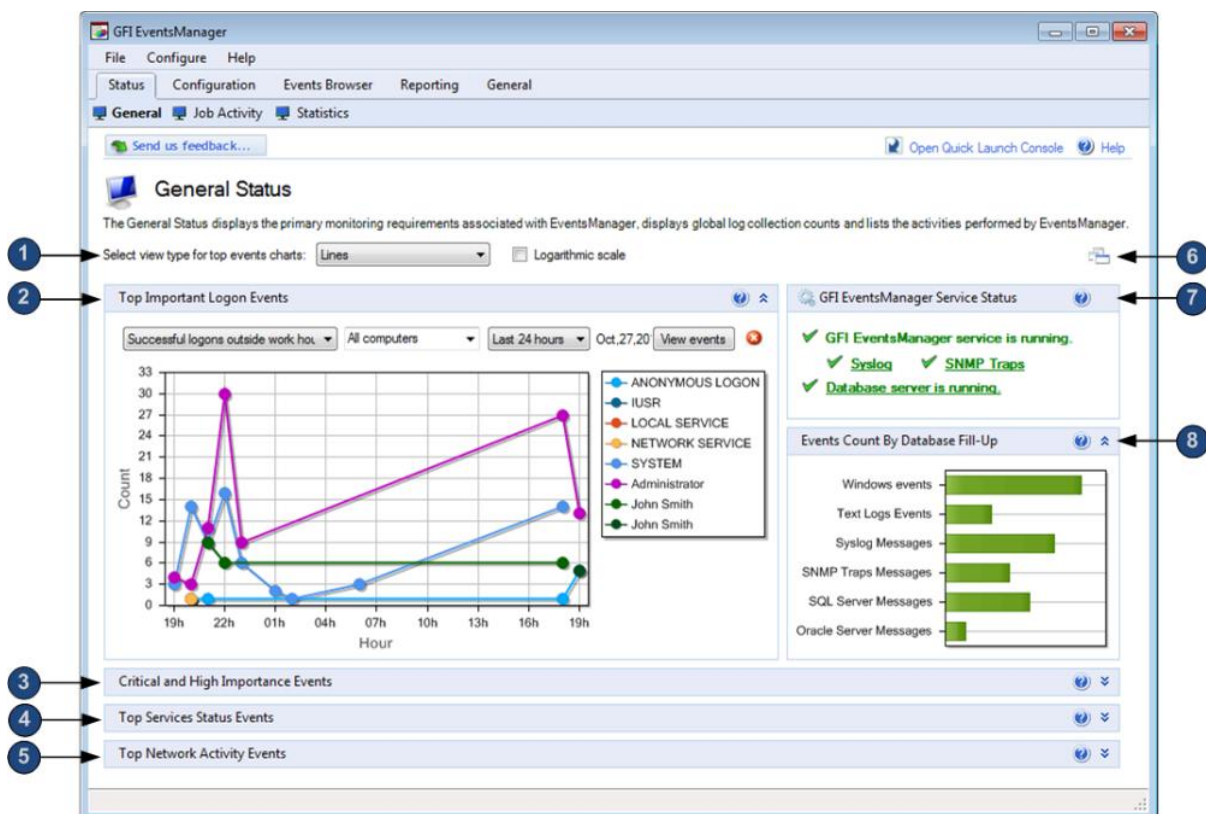


Screenshot 117 - Dashboard View Options

This chapter contains information about the following views:

- » General status view
- » Job Activity view
- » Statistics view

11.2 General status view



Screenshot 118 - GFI EventsManager Status: General view

To access the **General** view, go to **Status** tab ► **General**. This view is used to:


- » View the status of the GFI EventsManager event processing engine

- » Access statistical information such as the number of logon events, critical events and service status events.

The General view of the Status tab is made up of the sections described below:

Table 70 - Status monitoring: General view

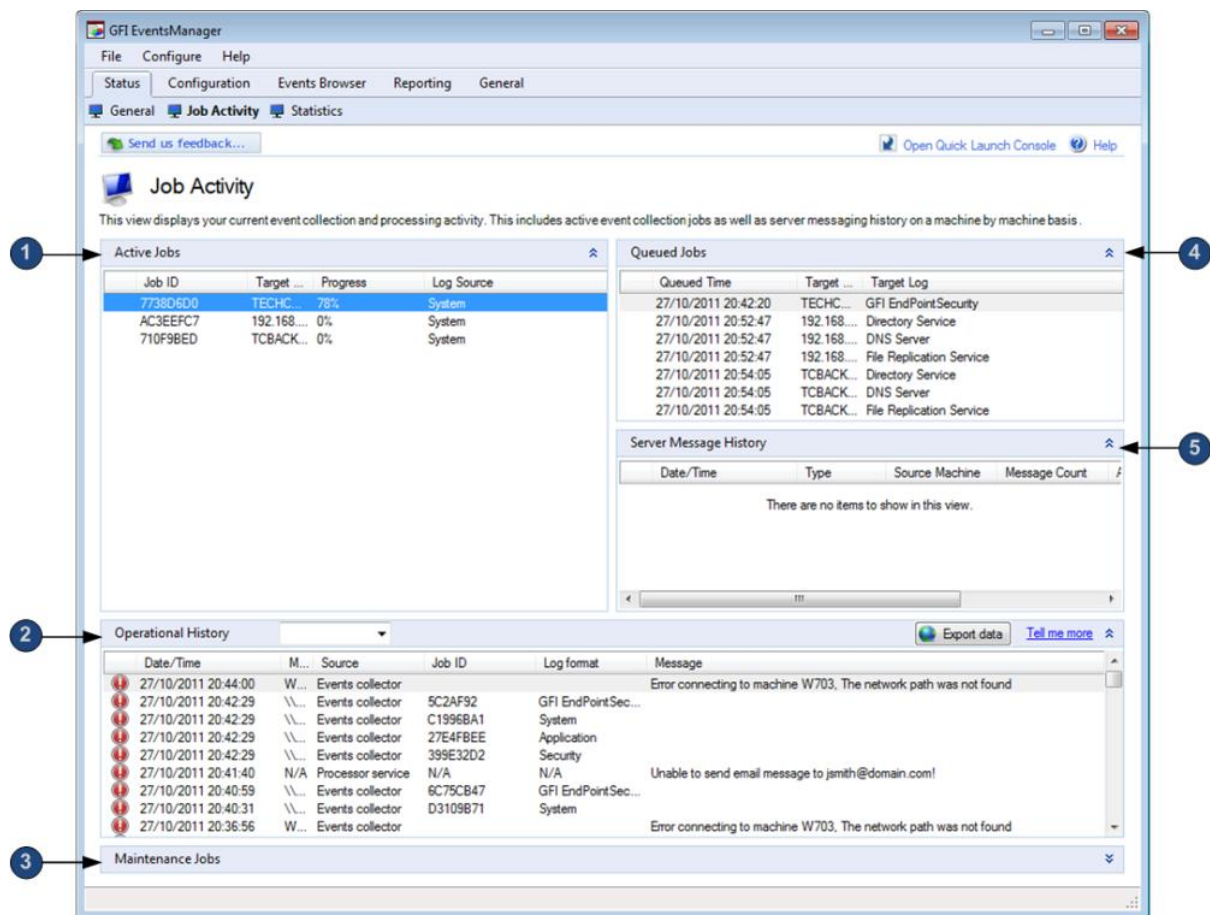
SECTION	DESCRIPTION
1	Use this section to select the chart type for top events.
2	<p>The Top Important Log Events section provides statistical information about:</p> <ul style="list-style-type: none"> » Top 10 successful Logon events outside working hours » Top 10 important Logon events during working hours » Top 10 failed Logon events. <p>Events in this section are filtered by:</p> <ul style="list-style-type: none"> » Machine: Select a machine or key in a machine name in the drop down list » Period: The time period when the events occurred (Last hour, Last 24 hours, Last 7 days or a specific date).
3	<p>The Critical and High Importance Events section provides statistical/graphical information about critical events collected from all event sources. This graph shows the event processing rules that collected and processed the events for a particular period.</p> <p>From the drop down lists, select the type of information to display. Select from:</p> <ul style="list-style-type: none"> » Grouping: Determines how events are grouped; such as Events, Computers, Computer groups, Events/Computers or Events/Computer groups » Event type: Select the type of data to display (Windows, W3C, Syslog, SNMP, SQL and Oracle audit) » Alert type: Specify the alert severity; such as All alerts, Critical or High » Period: Specify the time period when the events occurred (Last hour, Last 24 hours, Last 7 days or a specific date). <p>NOTE 1: This section also displays the vulnerability results monitored by GFI LanGuard.</p> <p>NOTE 2: For detailed information about the different types of important events shown in this graph, download the Microsoft Security Monitoring and Attack Detection Planning Guide from http://www.gfi.com/ms-security-mointoring-and-attack-detection-planning/.</p>
4	<p>The Top Service Status Events displays the top 10 services that caused the selected event. A service can generate events when:</p> <ul style="list-style-type: none"> » Terminated with an error » Failed to load » Failed to start » Timed out » Stopped » Started. <p>The graph shows the frequency of these events sorted by service type or\and by computer generating the event. Select a machine or service from the drop down lists or key in the required criteria to customize the graph results.</p> <p>NOTE: To collect services information, event sources must have Audit system events policy enabled. For more information, refer to Step 2: Enable additional auditing features.</p>

SECTION	DESCRIPTION
5	<p>The Top Network Activity Events section displays details of the top 10 network activities (inbound and outbound). Network activity consists of all type of traffic that is generated by various protocols including SMTP, HTTP, FTP and MSN traffic. The network activities displayed can be filtered by:</p> <ul style="list-style-type: none"> » Applications » Source Addresses » Destination Addresses » Computers » Ports » Users. <p>Select parameters from the drop down lists or key in the values to filter the type of chart displayed.</p> <p>NOTE 1: The network activity shown in the chart applies only to computers running Microsoft Windows Vista or later.</p> <p>NOTE 2: To collect network activities, event sources must have Object auditing and Process tracking enabled. For more information, refer to Step 2: Enable additional auditing features.</p>
6	<p>Click the Arrange Window icon  to automatically fit all graphs in the management console.</p>
7	<p>The GFI EventsManager Service Status is used to view:</p> <ul style="list-style-type: none"> » The operational status of GFI EventsManager service/event processing engine » The operational status of the Syslog server » The operational status of the SNMP Traps server » The operational status of the database server currently in use by GFI EventsManager. <p>NOTE: Click the service name to edit the service settings.</p>
8	<p>The Events Count By Database Fill-Up displays:</p> <ul style="list-style-type: none"> » The horizontal bars represent the number of events stored in the database backend, sorted by event log type » The date and time of the last backup » The date and time of the next scheduled backup. <p>The bar color turns from green to red as the database is populated with events.</p>



Double-click the graph to open the graph in a new window. When a 3D graph is selected, the new window allows you to rotate, zoom or resize the graph. Use the **Export to image** button to export the graph.

11.3 Job activity view



Screenshot 119 - GFI EventsManager Status: Job Activity view

To access the **Job Activity** view, go to **Status** tab ► **Job Activity**.

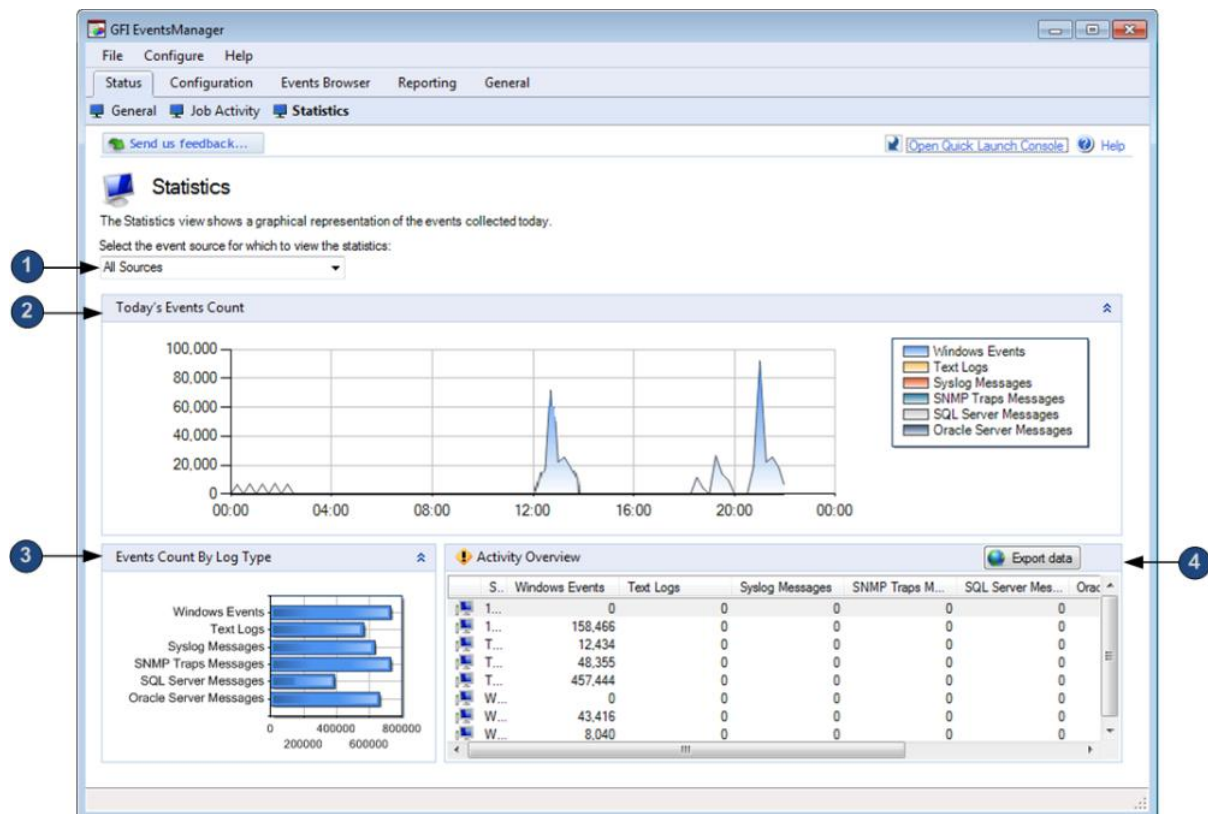
This view displays your current event collection and processing activity. This includes active event collection jobs as well as server messaging history on a machine by machine basis.

The information provided in this view is divided into the following dedicated sections:

Table 71 - Status monitoring: Job activity view

SECTION	DESCRIPTION
1	The Active Jobs section provides a list of all event collection jobs currently taking place on every event source/machine. The information provided includes the job progress as well as the Log Source from which events are being collected.
2	The Operational History section shows an audit trail of the event collection operations performed by GFI EventsManager. The information provided includes errors and information messages generated during the event collection process as well as the name of the log file that was being processed on the event source. NOTE: Operational history logs can be exported using the Export data button. For more information, refer to Operational History .
3	The Maintenance Jobs section displays the progress of maintenance jobs that have been created through Database Operations . The information provided includes the job description, start time and state.
4	The Queued Jobs section provides a list of all pending event collection jobs on a machine by machine basis. The information provided includes the event source from which events will be collected as well as the queuing time and type of log to collect.
5	The Server Message History section displays a list of all server messages (SNMP Traps and Syslog) that were received by GFI EventsManager. The information provided includes the total number of messages sent by every event source, message count and the date/time when the last message was received.

11.4 Statistics view



Screenshot 120 - GFI EventsManager Status: Statistics view

To access the **Statistics** view, go to **Status** tab ► **Statistics**.

The **Statistics** view is used to display the daily event activity trends and statistics of a particular computer or entire network. The information provided in this view is divided into the following dedicated sections:

Table 72 - Status monitoring: Statistics view

SECTION	DESCRIPTION
1	Use this drop-down menu to select what information is displayed. Select between All sources or select specific sources to view their information accordingly.
2	The Today's Events Count graphically represents the daily event collection trend on a machine by machine basis as well as on a network by network basis. A color scheme is used to differentiate between Windows, W3C, Syslog and SNMP Traps events.
3	The Events Count By Log Type represents the number of Windows, W3C, Syslog and SNMP Traps events collected by GFI Events Manager from a particular machine or network.
4	The Activity Overview section provides information about: <ul style="list-style-type: none"> » The total number of Windows, W3C, Syslog and SNMP Traps events processed on a machine by machine basis » The date/time of the last event collection performed from every machine.

12 Database Operations

12.1 Introduction

The **Database Operations** module in GFI EventsManager provides advanced functionality allowing administrators to:

- » Centralize events collected by other remote GFI EventsManager instances into one database backend.
- » Optimize GFI EventsManager performance by actively controlling database backend growth hence keeping it in good shape.
- » Import and export data to and from GFI EventsManager version 8.x installations without data inconsistencies.
- » Import and export events to and from a storage folder minimizing data loads from the database.

This chapter includes sections containing information about:

- » [Why database maintenance?](#)
- » [Creating a new database backend](#)
- » [Configuring Database Operations](#)
- » [Creating maintenance jobs](#)
- » [Editing existing maintenance jobs](#)

12.2 Why database maintenance?

Periodical database maintenance is essential in preventing excessive data growth in the database backend. A database which is large in size drastically affects the performance of GFI EventsManager; events browsing will be slower and queries will take longer to execute.

Through GFI EventsManager, a number of database operations, referred to as maintenance jobs, can be carried out on the database backend. These include:

Table 73 - Available database operations

DATABASE OPERATION	DESCRIPTION
Import from file	The Import from file job enables you to import data as part of the data centralization process. Only files created from an Export to file job are supported for import.
Export to file	The Export to file job enables you to export data into a file to import into another instance of GFI EventsManager or to archive in an external storage media for safekeeping.
Import from SQL Server database	The Import from SQL Server database job enables you to import events collected from an older version of GFI EventsManager.
Import from legacy files	The Import from legacy files job enables you to import configuration files exported from an older version of GFI EventsManager.
Import from legacy file storage	The Import from legacy file storage job enables you to import data archived by a previous version of GFI EventsManager. Archive files were exported in a special file format utilized by GFI EventsManager.

12.2.1 Consolidation of events in a WAN environment

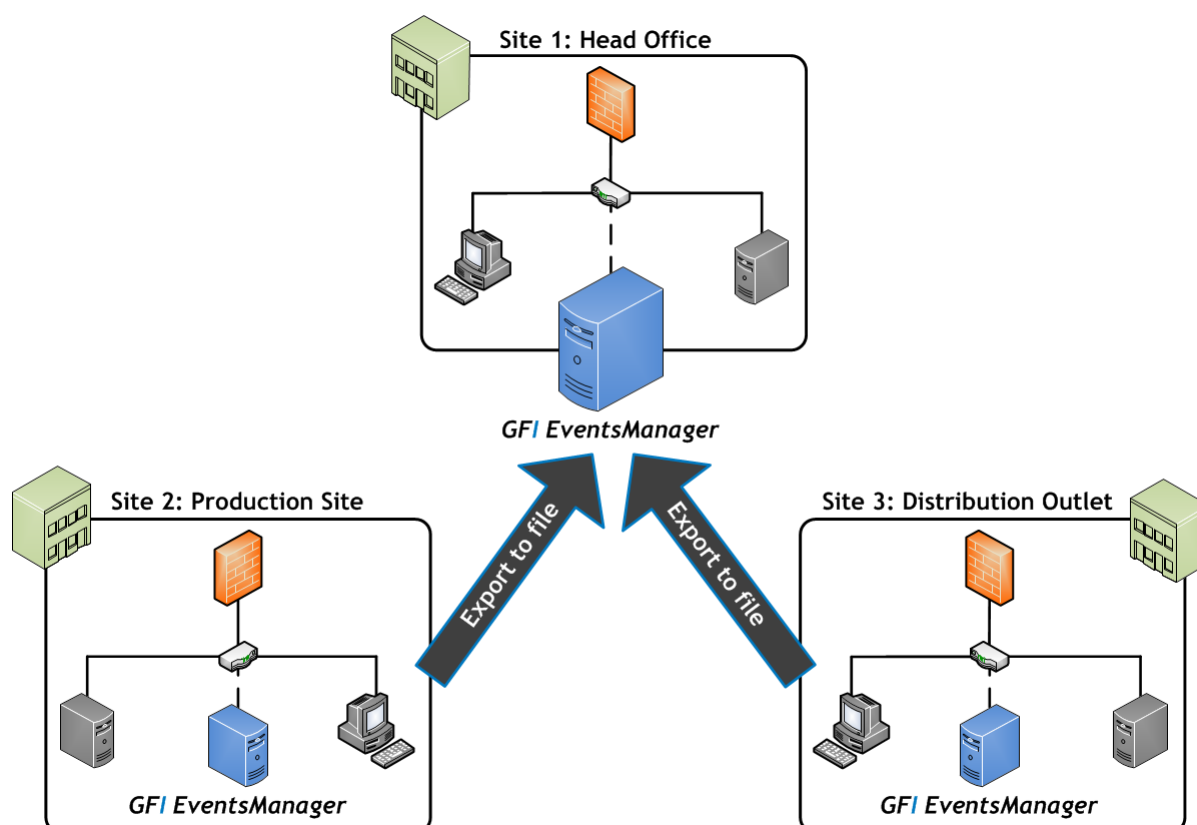


Figure 9: Consolidation of events in a WAN environment

In the case of organizations with remote geographical sites, Database Operations can be used to consolidate all or part of the events data collected in remote sites on to one central database. This is achieved using the **Export to file** feature through which GFI EventsManager compresses and encrypts the file as well as export the file to be processed to a central location. The **Import to file** job is executed at the central location, importing the events from the remote site into the central database.

Events for the remote site can then be viewed through the **Events Browser**. Reports with information relevant to the remote site can also be generated using data from the central database.

12.3 Creating a new database backend

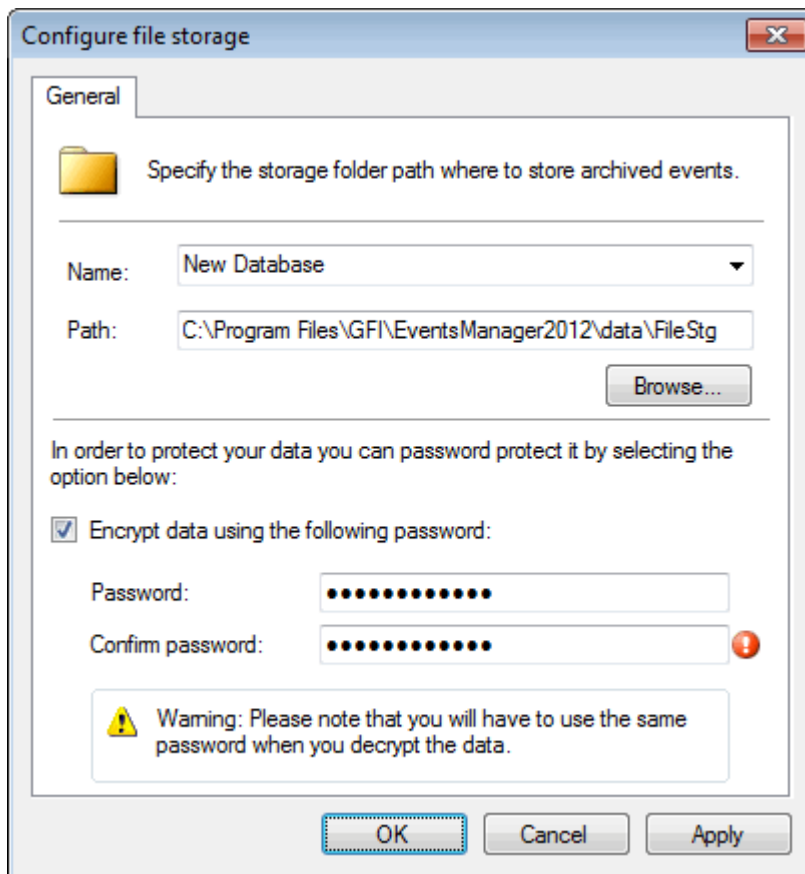
GFI EventsManager makes use of an internal storage system which allows great scalability with its fast read/write capabilities even when processing high volumes of data. You may have as many databases as required. The Events Browser enables you to easily switch from on database to another, allowing viewing events from archived databases.

As an example, you can create a new database for every month or year depending on the volume of event logs that are processed.

You can also encrypt new databases before starting to use them. The live database can only be encrypted though `esmdlibm.exe`. For more information, refer to [Using esmdlibm.exe](#).

To create a new database:

1. Click **Configuration** tab ► **Options**.
2. From **Configurations**, click **File storage** ► **Configure file storage...**



Screenshot 121 - Archive Storage Folder dialog

3. Specify or browse for the path for the new database.
4. Specify the name for the new database.
5. (Optional) Select **Encrypt data using the following password** and specify an encryption password.



Indicates that the specified passwords do not match.



Encrypting the live database is not supported from the GFI EventsManager Management Console. To encrypt the live database, use **esmdlibm.exe**. For more information, refer to [Using Esmdlibm.exe](#).

6. Click **OK** to save your settings.

12.3.1 Switching databases

To switch from one database to another:

1. From **Archive storage folder** dialog, click **Browse** or specify the path to the database you want to load.
2. From **Name** drop-down menu, select the database.
3. (Optional) Enable/Disable encryption.



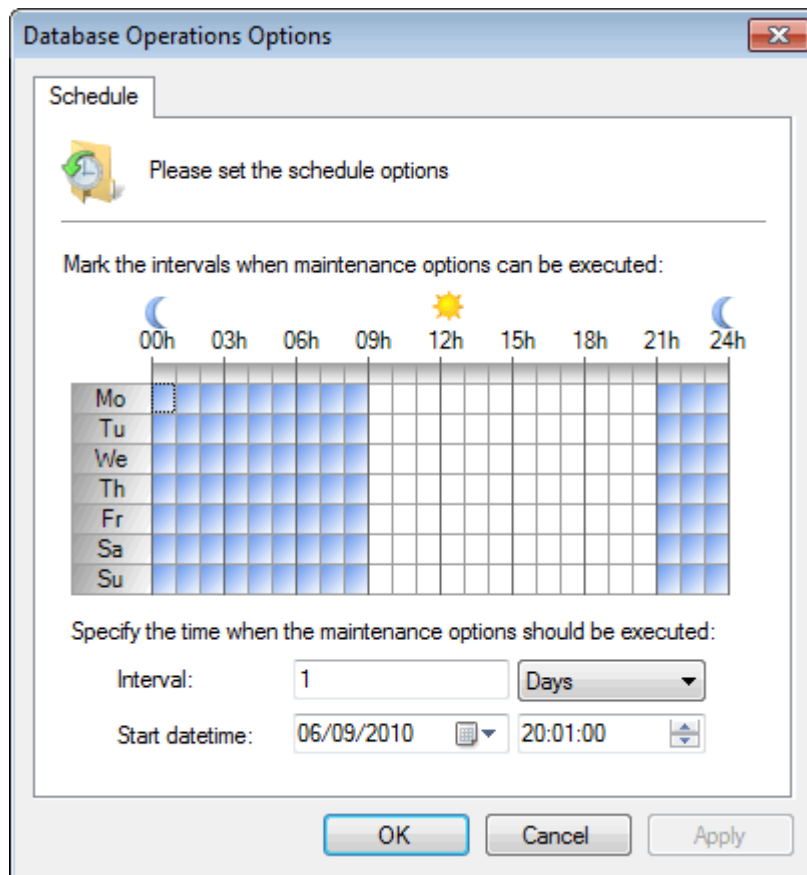
GFI EventsManager supports encryption of offline databases through the Management Console.

4. Click **OK** to save your settings.

12.4 Configuring Database Operations

To configure Database Operations:

1. Click **Configuration** tab ► **Options**.
2. From **Configurations**, right-click **Database Operations** and select **Properties**.



Screenshot 122 - Database Operations Options dialog

3. From the **Database Operations Options** dialog, configure the tabs described below:

Table 74 - Configuring database operations

TAB	DESCRIPTION
General	Specify the unique identifier by which this instance of GFI EventsManager will be identified on the network. This identifier is used as part of the export file-name during Export to file operations.
Schedule	Through the Schedule tab, configure: specify: <ul style="list-style-type: none">» Hours of the day during which maintenance jobs can be executed» The interval in hours/days with which maintenance jobs will be executed» The scheduled date/time when maintenance jobs will start being executed.

4. Click **OK** to save your settings.

12.5 Creating maintenance jobs

With GFI EventsManager you can schedule maintenance jobs to be executed on a specific day, at a specific time and at specific intervals.



Database maintenance operations may require high utilization of resources. This can degrade server and GFI EventsManager performance. Schedule maintenance jobs to be executed after office hours to maximize the availability of your system resources and avoid any possible workflow disruptions to workflow.

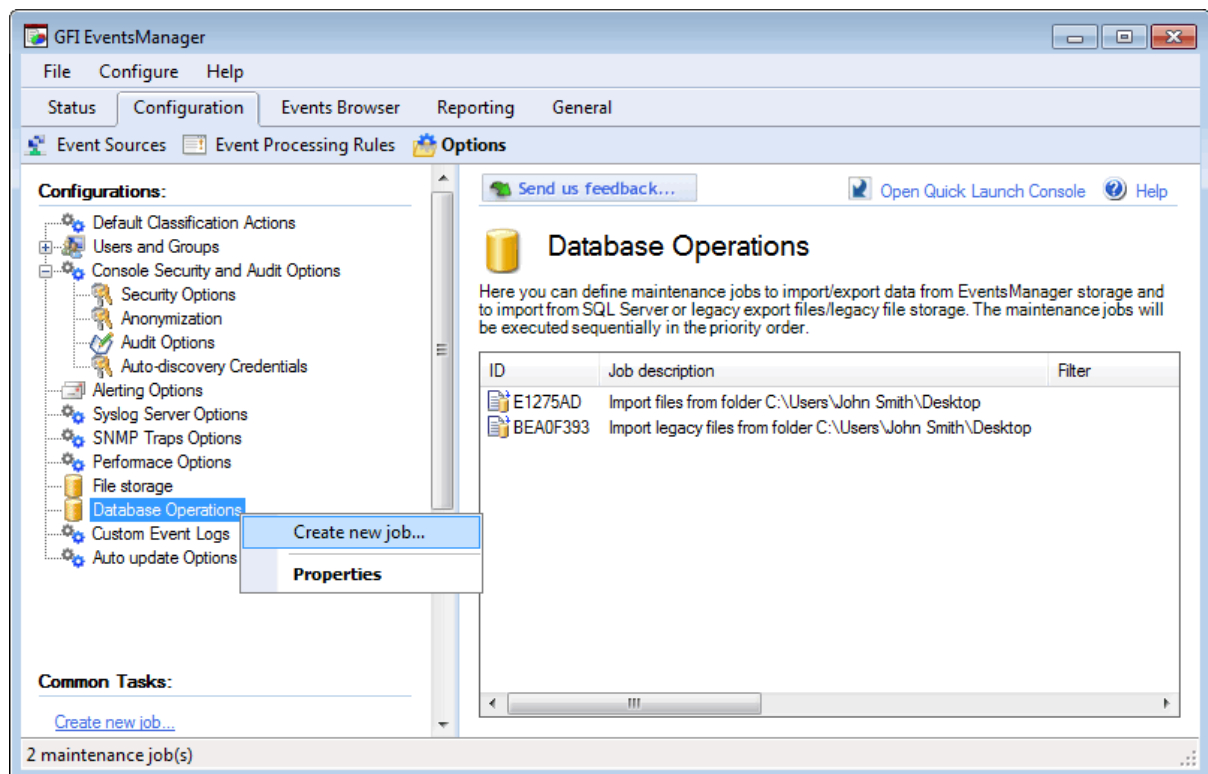
GFI EventsManager supports five types of database operations. For more information, refer to the following sections in this chapter:

- » [Import from file](#)
- » [Export to file](#)
- » [Import from SQL Server database](#)
- » [Import from legacy files](#)
- » [Import from legacy file storage](#)

12.5.1 Import from file

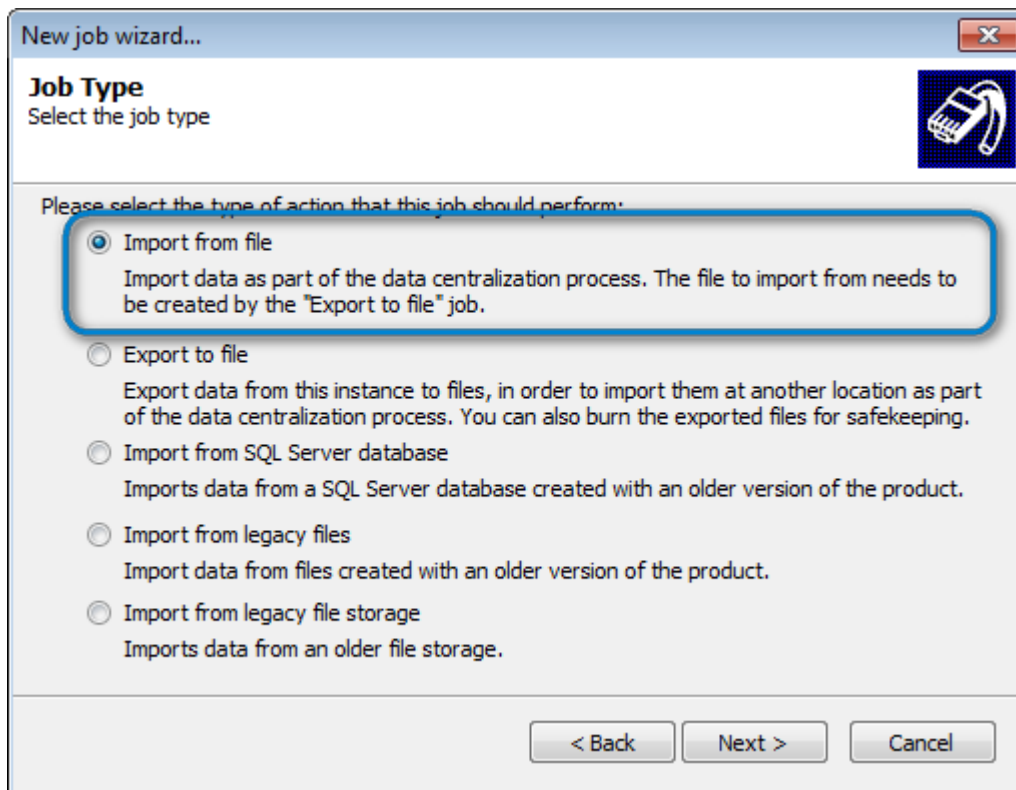
To create an Import from file job:

1. Click **Configuration** tab and select **Options**.



Screenshot 123 - Creating a new Database Operation

2. From **Configurations**, right-click **Database Operations** and select **Create new job...**



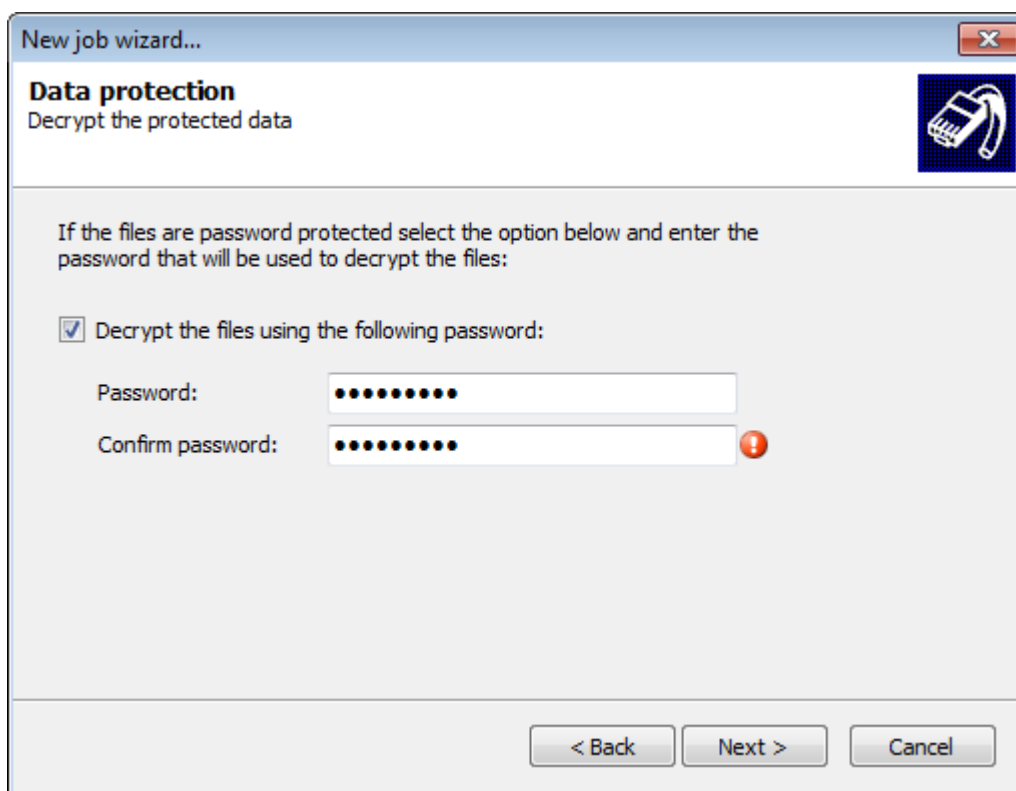
Screenshot 124 - Import from File

3. Click **Next** at the wizard welcome screen and select **Import from file** as the job type. Click **Next**.

4. Specify the full path or browse for the file to import. Click **Next**.



Only files exported from GFI EventsManager can be imported.



Screenshot 125 - Import from file: Decrypt

5. If the exported events are encrypted, select **Decrypt the files using the following password** and specify the encryption password. Click **Next**.

6. (Optional) Specify filtering conditions to filter out unwanted data. Leave it blank to import everything. Click **Next**.



For more information, refer to [Defining Restrictions](#).

7. Select when the job is executed. The table below describes the available options:

Table 75 - Database operations: Schedule options

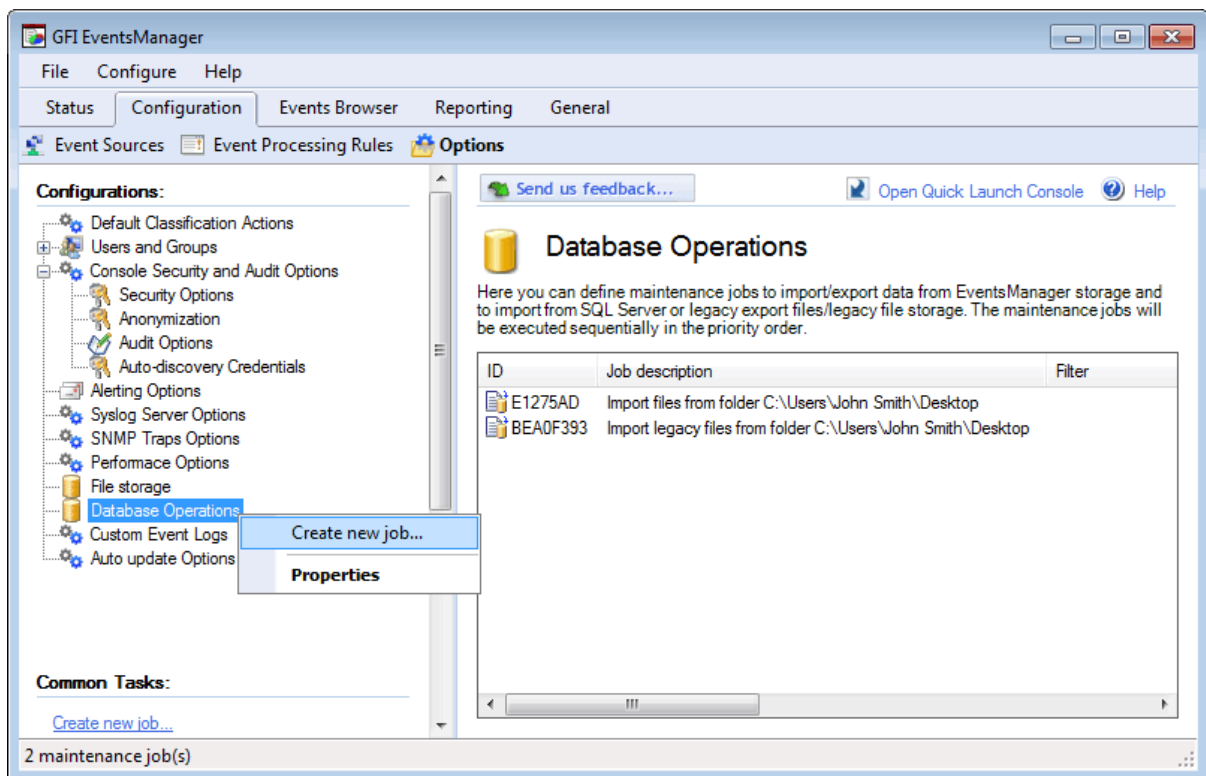
OPTION	DESCRIPTION
Schedule job	The job will be saved and executed according to the database operations schedule.
Run the job now	Job is executed immediately. Unscheduled jobs only run once.

8. Click **Finish**.

12.5.2 Export to file

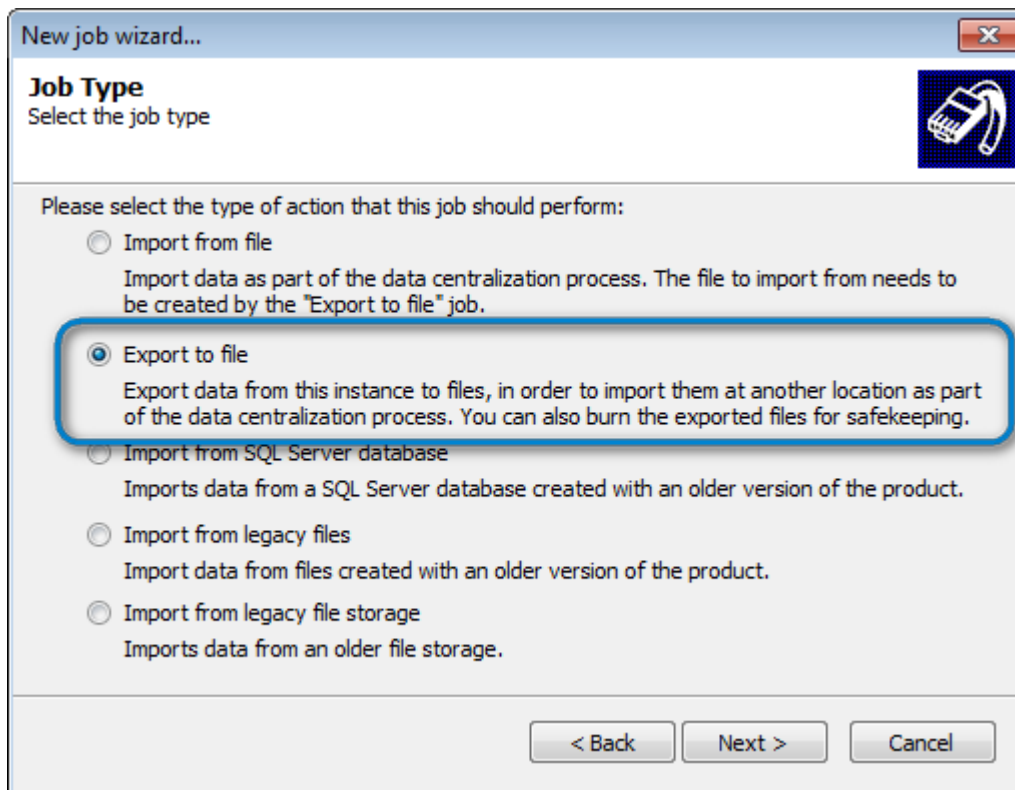
To create an export to file job:

1. Click **Configuration** tab and select **Options**.



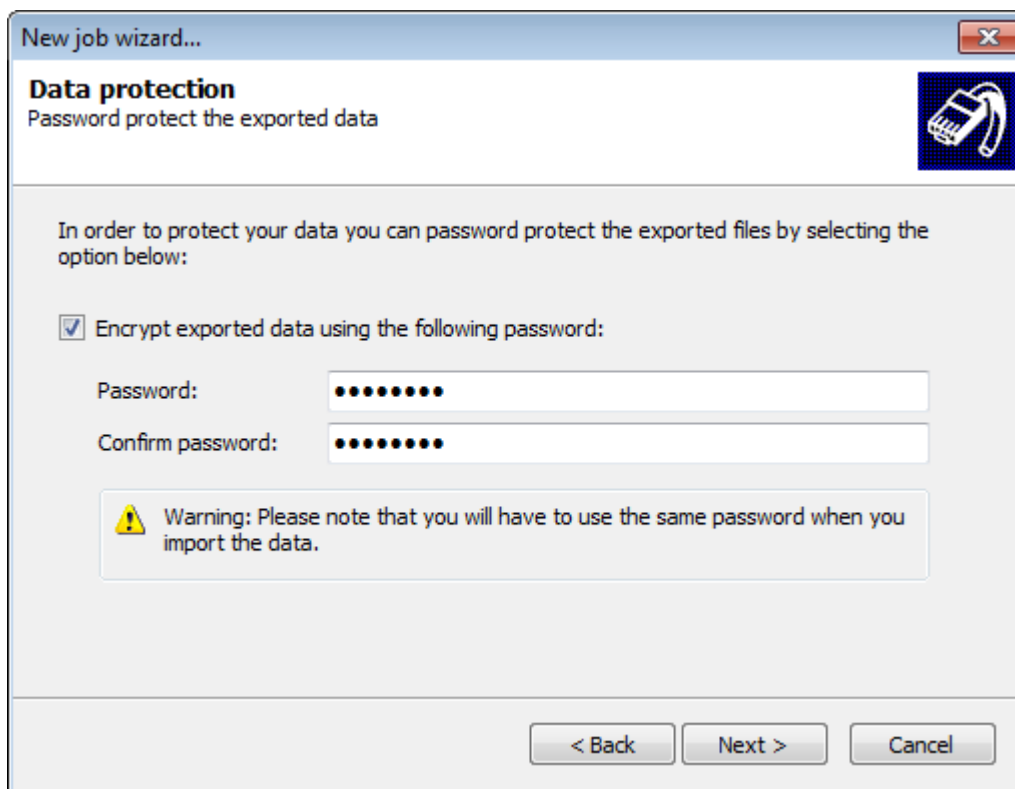
Screenshot 126 - Creating a new Database Operation

2. From **Configurations**, right-click **Database Operations** and select **Create new job...**



Screenshot 127 - Export to File

3. Click **Next** at the wizard welcome screen and select **Export to file** as the job type. Click **Next**.
4. Specify or browse for the location where the exported file will be saved. Click **Next**.



Screenshot 128 - Export to File: Encrypt exported data

5. (Optional) Select **Encrypt exported data using the following password** and specify an encryption key to protect your exported data. Click **Next**.
6. (Optional) Specify filtering conditions to filter out unwanted data. Leave it blank to export all the data in the database. Click **Next**.

7. Select when the job is executed. The table below describes the available options:

Table 76 - Database operations: Schedule options

OPTION	DESCRIPTION
Schedule job	The job will be saved and executed according to the database operations schedule.
Run the job now	Job is executed immediately. Unscheduled jobs only run once.

8. Click **Finish**.

Export filename

The convention used by GFI EventsManager to name the export file is shown and described below:

[ESM ID]_[Job ID]_[Date From]_[Date To].EXP

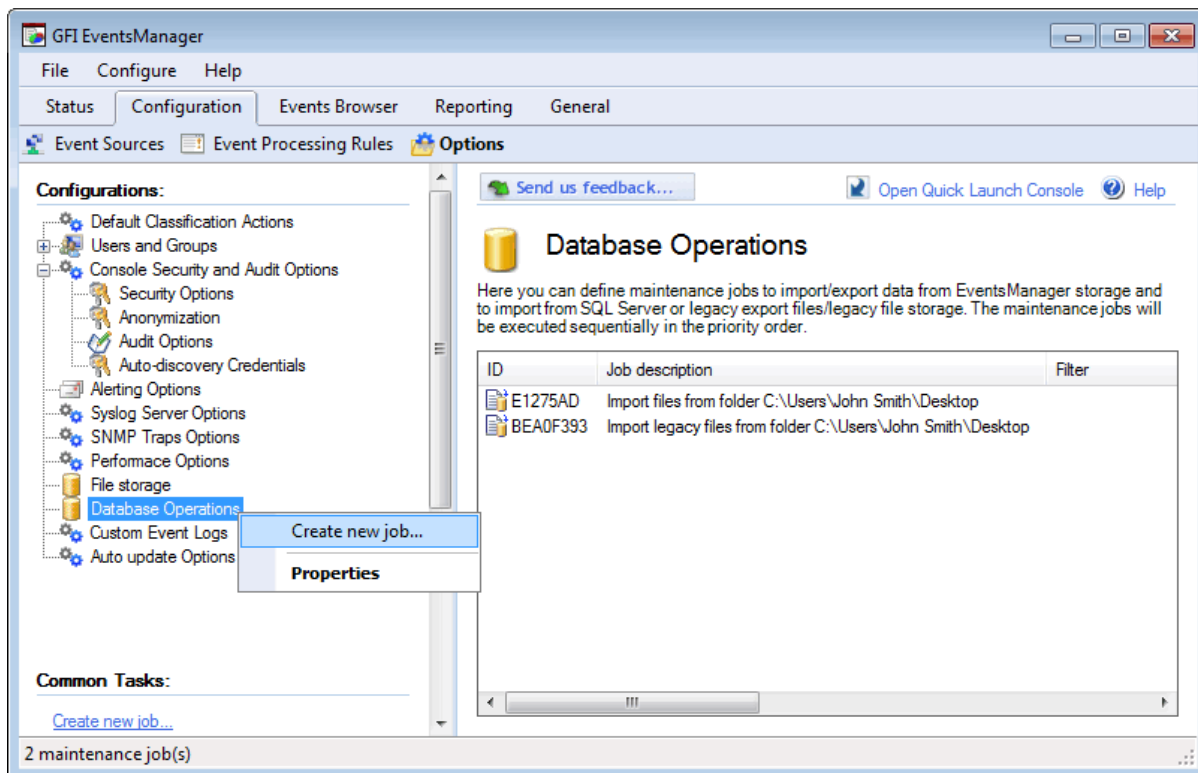
Table 77 - Table 78 - Database operations: Export file name structure

SECTION	DESCRIPTION
ESM ID	Refers to the unique identifier given to each GFI EventsManager instance running in the organization.
Job ID	Refers to the unique identifier given to each maintenance job created.
Date From	Refers to the date of the earliest event exported.
Date To	Refers to the date of the latest event exported.
.EXP	This is the file extension given to all export files.

12.5.3 Import from SQL Server database

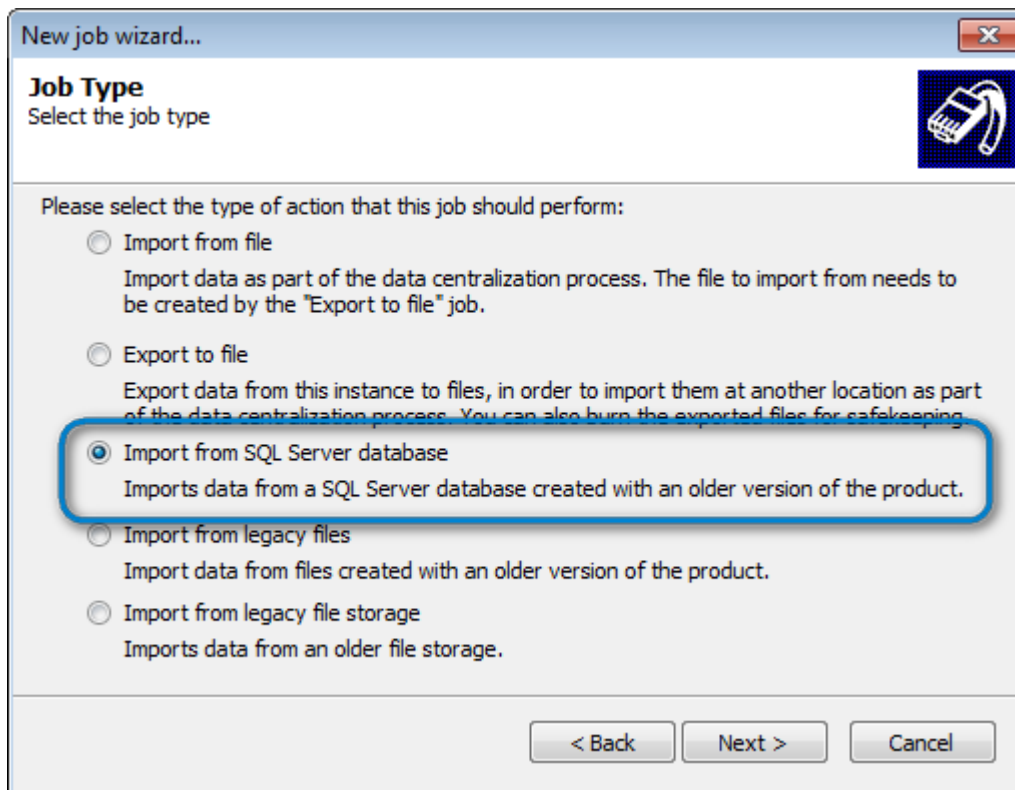
To create an import from SQL Server database job:

1. Click **Configuration** tab and select **Options**.



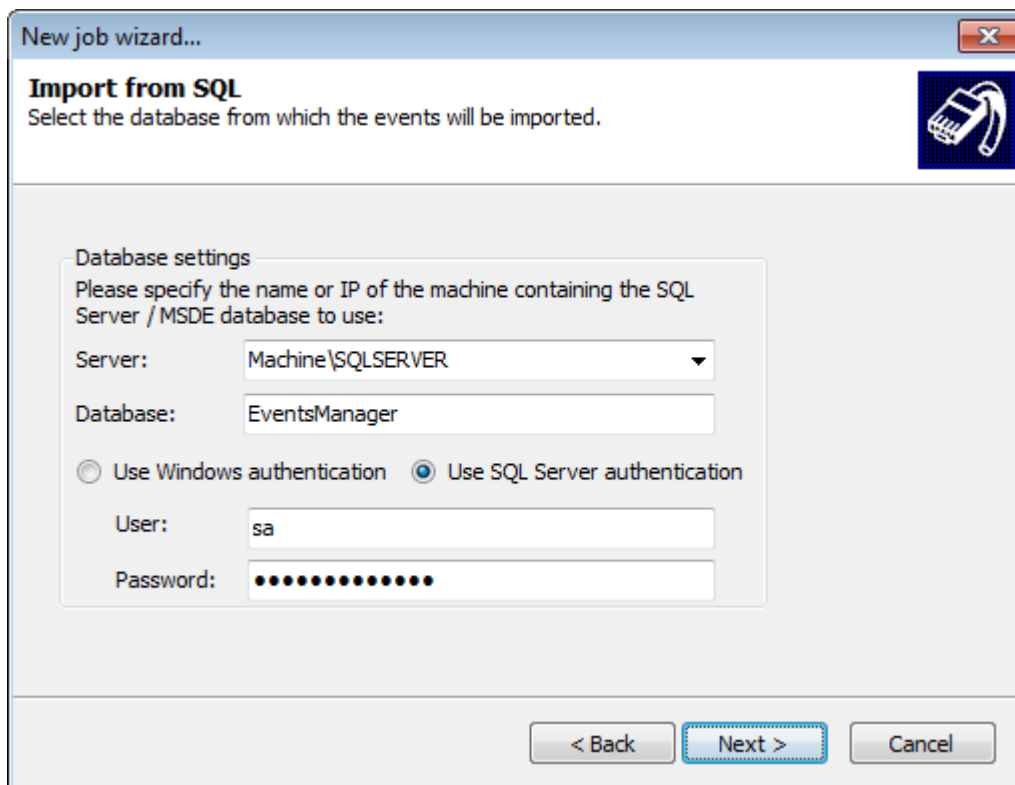
Screenshot 129 - Creating a new Database Operation

2. From **Configurations**, right-click **Database Operations** and select **Create new job...**



Screenshot 130 - Import from SQL Server database

3. Click **Next** at the wizard welcome screen and select **Import from SQL Server database** as the job type. Click **Next**.



Screenshot 131 - Import from SQL Server database: Select the database to import

4. Select the SQL Server and the respective database to import and specify the SQL Server login credentials. Click **Next**.

New job wizard...

Anonymized data
Decrypt anonymized data

Decrypt anonymized data

☒ Enable decryption

Decryption key: *****
Confirm key: *****

☒ Use secondary decryption key

Decryption key: *****
Confirm key: *****

< Back Next > Cancel

Screenshot 132 - Import from SQL Server database: Decrypt anonymized data

5. If the target database to import is anonymized, select **Enable decryption** and specify the encryption password used to protect the database.
6. (Optional) If the database is protected by two encryption passwords, select **Use secondary decryption key** and specify the second encryption password. Click **Next**.
7. (Optional) Specify filtering conditions to filter out unwanted data. Leave it blank to export all the data in the database. Click **Next**.
8. Select when the job is executed. The table below describes the available options:

Table 79 - Database operations: Schedule options

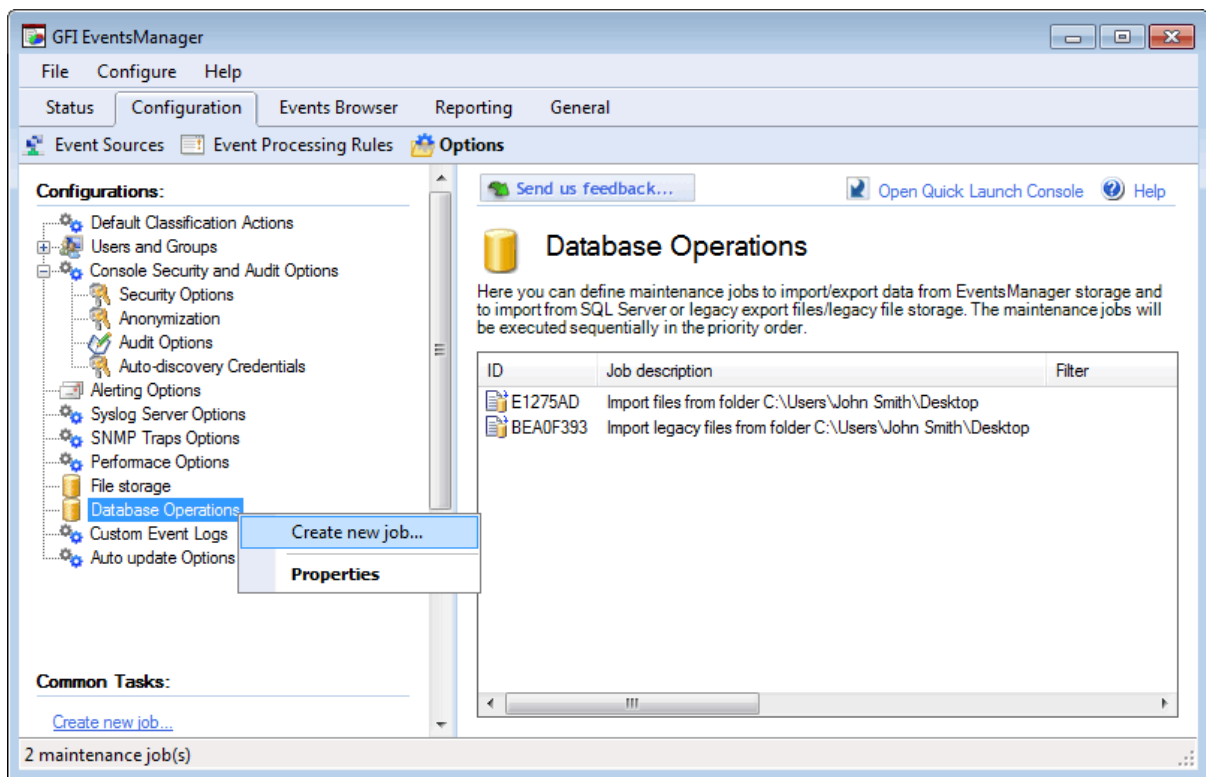
OPTION	DESCRIPTION
Schedule job	The job will be saved and executed according to the database operations schedule. For more information, refer to Configuring database operations .
Run the job now	Job is executed immediately. Unscheduled jobs only run once.

9. Click **Finish**.

12.5.4 Import from legacy files

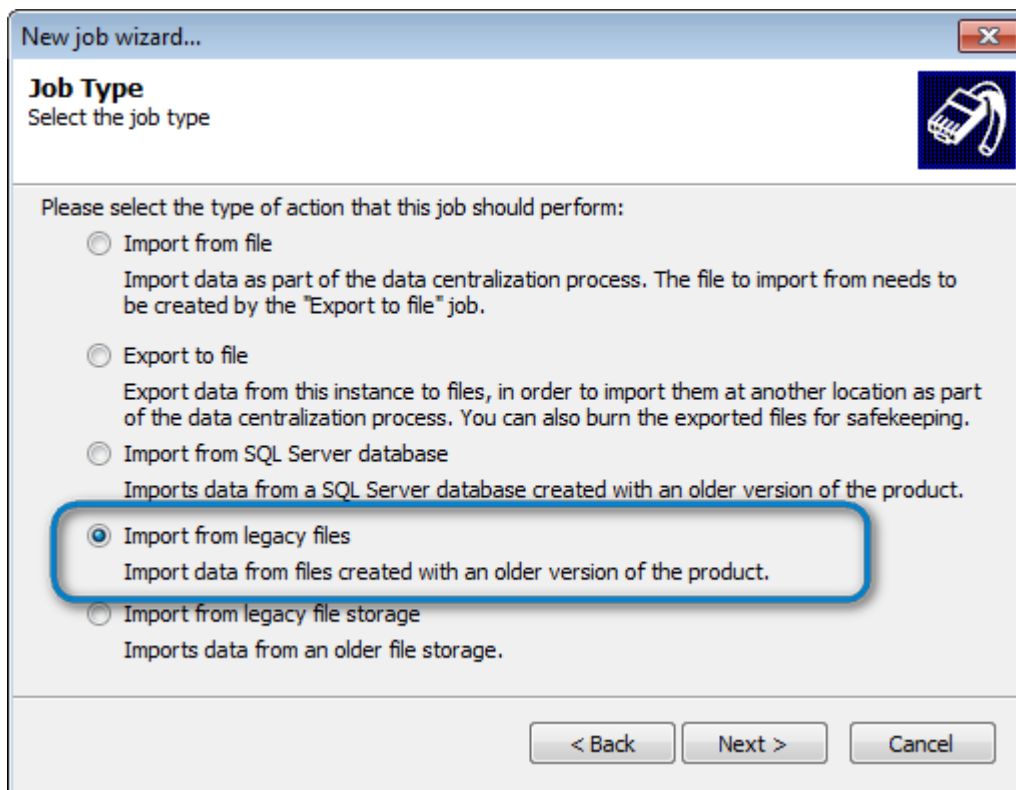
To create an import from legacy files job:

1. Click **Configuration** tab and select **Options**.



Screenshot 133 - Creating a new Database Operation

2. From **Configurations**, right-click **Database Operations** and select **Create new job...**



Screenshot 134 - Import from legacy files

- Click **Next** at the wizard welcome screen and select **Import from legacy files** as the job type. Click **Next**.
- Specify the location or browse for the legacy file to import. Click **Next**.
- (Optional) If the legacy files are encrypted, select **Decrypt the files using the following password** and specify the encryption password. Click **Next**.

6. (Optional) If the legacy files were anonymized, select **Enable decryption** and specify the decryption password.
7. (Optional) If the legacy file is protected by two anonymization passwords, select **Use secondary decryption key** and specify the second password. Click **Next**.
8. (Optional) Specify filtering conditions to filter out unwanted data. Leave it blank to export all the data in the database. Click **Next**.
9. Select when the job is executed. The table below describes the available options:

Table 80 - Database operations: Schedule options

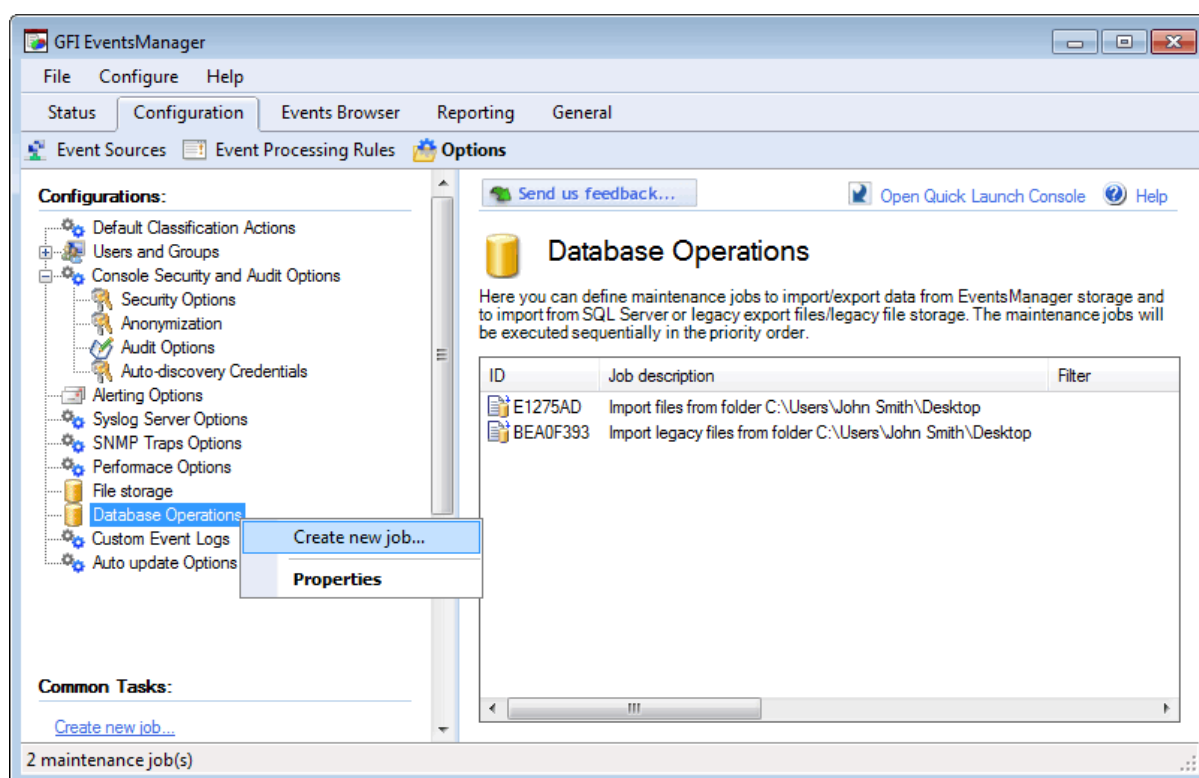
OPTION	DESCRIPTION
Schedule job	The job will be saved and executed according to the database operations schedule. For more information, refer to Configuring database operations .
Run the job now	Job is executed immediately. Unscheduled jobs only run once.

10. Click **Finish**.

12.5.5 Import from legacy file storage

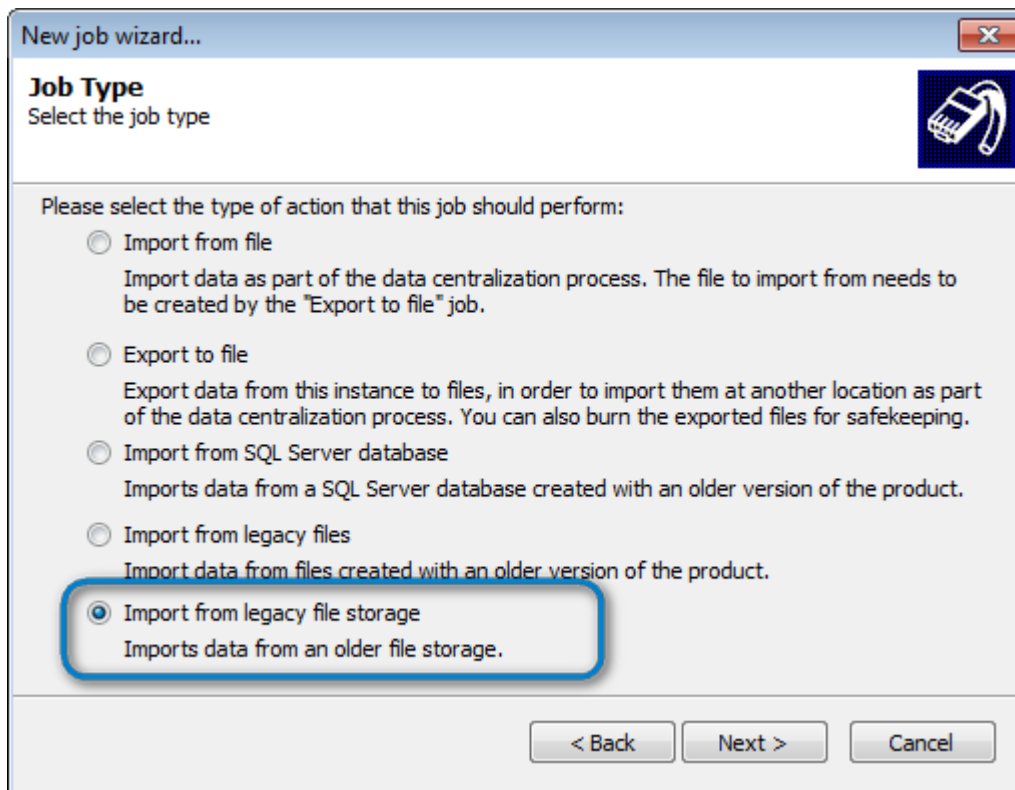
To create an import from legacy files job:

1. Click **Configuration** tab and select **Options**.



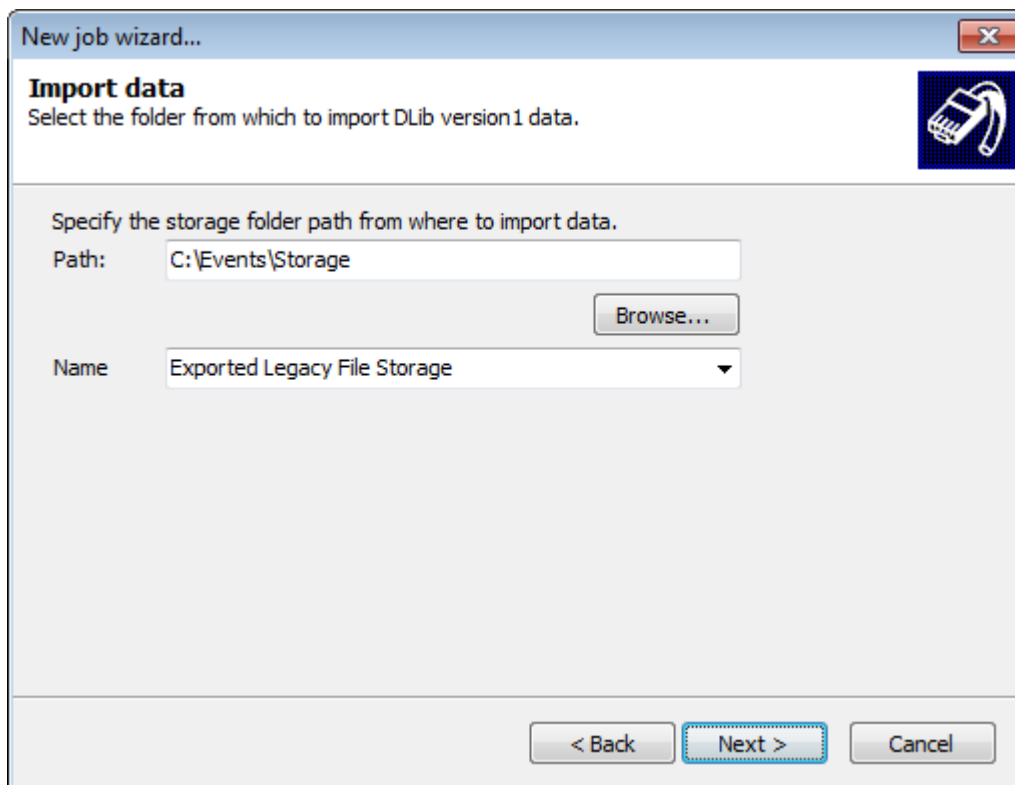
Screenshot 135 - Creating a new Database Operation

2. From **Configurations**, right-click **Database Operations** and select **Create new job...**



Screenshot 136 - Import from legacy file storage

3. Click **Next** at the wizard welcome screen and select **Import from legacy file storage** as the job type. Click **Next**.



Screenshot 137 - Import from legacy file storage: Select file to import

4. Specify the path and the file name of the exported legacy file. Click **Next**.
5. (Optional) If the data is anonymized, select **Enable decryption** and specify the password.
6. (Optional) If the data is encrypted by two passwords, select **Use secondary decryption key** and key in the secondary password. Click **Next**.

7. (Optional) Specify filtering conditions to filter out unwanted data. Leave it blank to export all the data in the database. Click **Next**.

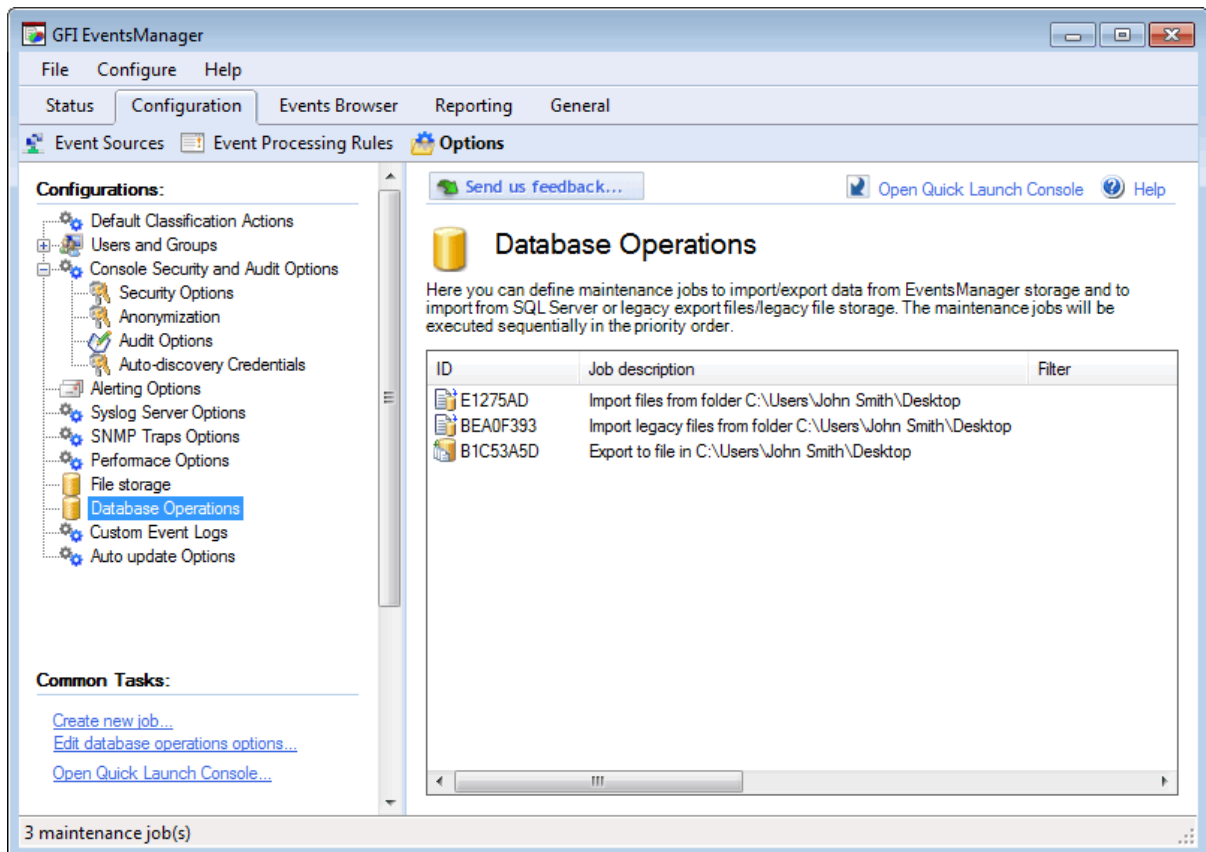
8. Select when the job is executed. The table below describes the available options:

Table 81 - Database operations: Schedule options

OPTION	DESCRIPTION
Schedule job	Job is saved and executed according to the database operations schedule. For more information, refer to Configuring database operations .
Run the job now	The job will be executed immediately. Unscheduled jobs only run once.

9. Click **Finish**.

12.6 Editing existing maintenance jobs



Screenshot 138 - Viewing scheduled maintenance jobs

To view maintenance jobs created:

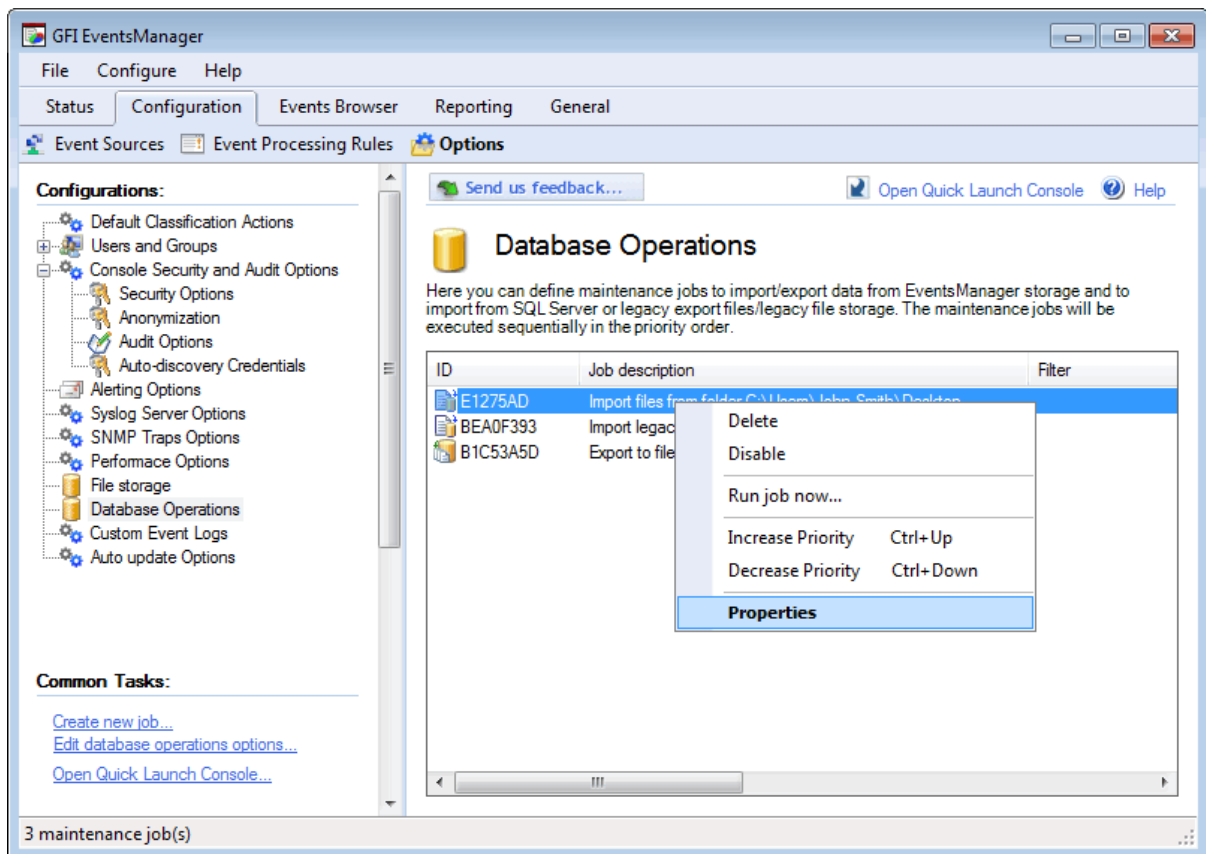
1. Click **Configuration** tab and select **Options**.
2. From the left pane, select the **Database Operations** node. Scheduled maintenance jobs will be displayed in the right pane.

12.6.1 Job activity status

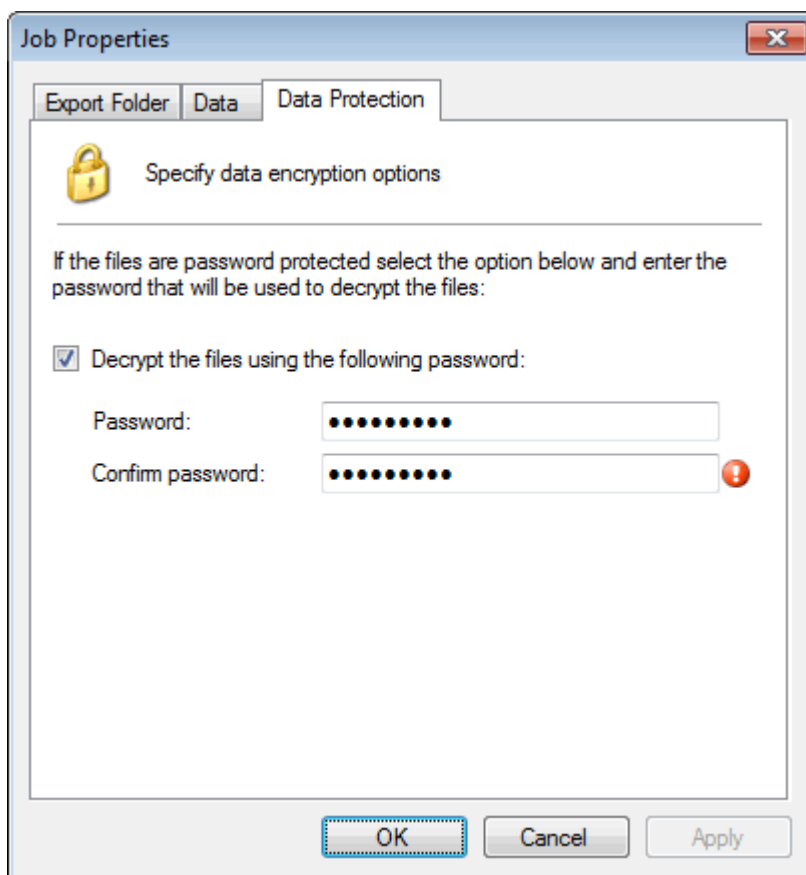
To view the progress of maintenance jobs that are being processed click **Status** tab and select the **Job Activity** dashboard view. The status of all maintenance jobs will be displayed in the **Maintenance Jobs** section.

You can make changes to maintenance job parameters for jobs scheduled.

1. Click **Configuration** tab and select **Options**.
2. From the left pane, select the **Database Operations** node.
3. From the right pane, right-click maintenance job to edit and select **Properties**.



Screenshot 139 - Editing a maintenance job



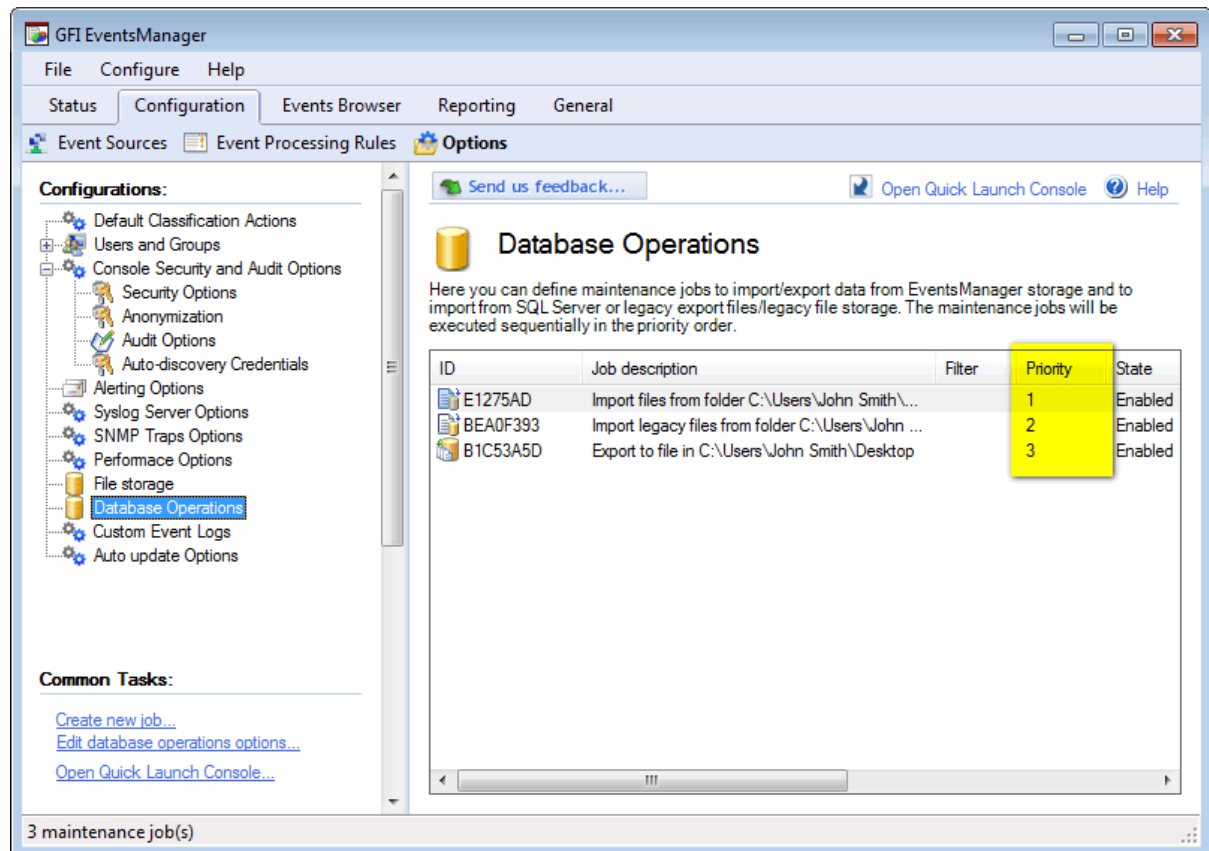
Screenshot 140 - Example dialog to edit a scheduled job

4. Configure the tabs described in the table below:

Table 82 - Database operations: Schedule options

TAB	DESCRIPTION
Export/Import Folder	Select the folder from where to import or where to export data.
Data	Configure conditions to filter event logs.
Data Protection	Enable/disable encryption. Specify a password to protect exported/imported data.

12.6.2 Changing maintenance job priority



Screenshot 141 - Maintenance job priorities

By default maintenance jobs are executed according to the sequence with which the jobs are created (First-in-First-out). Thus the priority of maintenance jobs is determined by the sequence in which jobs are executed.

To increase or decrease the priority of a maintenance job:

1. Click **Configuration** tab and select **Options**.
2. From the left pane, select the **Database Operations** node.
3. From the right pane, right-click the maintenance job and select **Increase Priority** or **Decrease Priority** accordingly.

12.6.3 Deleting a maintenance job

Scheduled maintenance jobs awaiting execution can also be deleted.

1. Click **Configuration** tab and select **Options**.
2. From the left pane, select the **Database Operations** node.
3. From the right pane, right-click on the maintenance job to delete and select **Delete**.



Before deleting maintenance jobs ensure that before deleting data, all data is backed up.

13 Miscellaneous

This chapter includes sections containing information about:

- » [Enabling permissions on event sources manually](#)
- » [Enabling permissions on event sources automatically](#)
- » [Disabling UAC to scan event sources](#)
- » [Command line tools](#)
- » [Auto updating GFI EventsManager](#)
- » [Product licensing](#)
- » [Version information](#)

13.1 Enabling permissions on event sources manually

This section describes how to configure permissions and ports that are required by GFI EventsManager manually. This process has to be done on each machine to scan. This section contains information about:

- » [Microsoft Windows XP](#)
- » [Microsoft Windows Vista](#)
- » [Microsoft Windows 7](#)
- » [Microsoft Windows Server 2003](#)
- » [Microsoft Windows Server 2008 \(including R2\)](#)

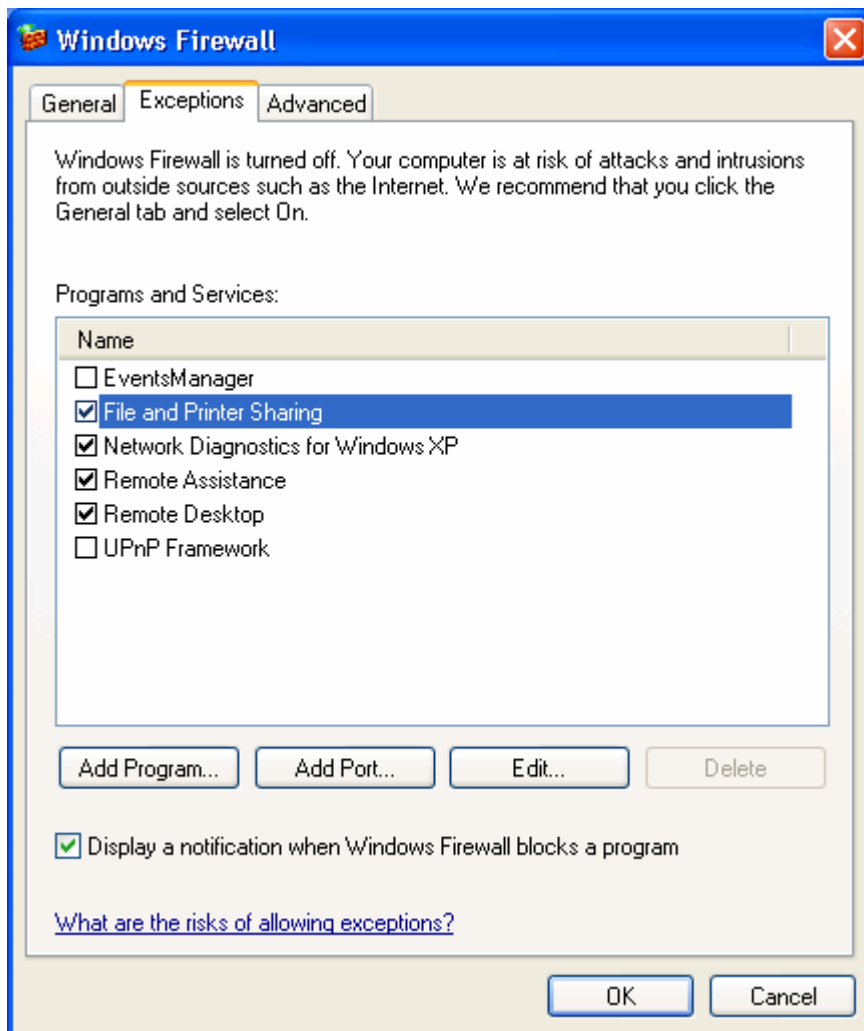


In a Windows 2003 or 2008 Active Directory environment, settings can be deployed automatically via Group Policy Object (GPO). For more information refer to [Enabling permissions on event sources automatically](#).

13.1.1 Microsoft Windows XP

To enable permissions and open the required ports on Microsoft Windows XP target machines:

1. Click **Start ► Control Panel ► Windows Firewall ► Exceptions** tab.



Screenshot 142 - Firewall rules on Microsoft Windows XP

2. Enable File and Printer Sharing from the Programs and Services list.
3. Click **OK** to apply changes and close.

13.1.2 Microsoft Windows Vista

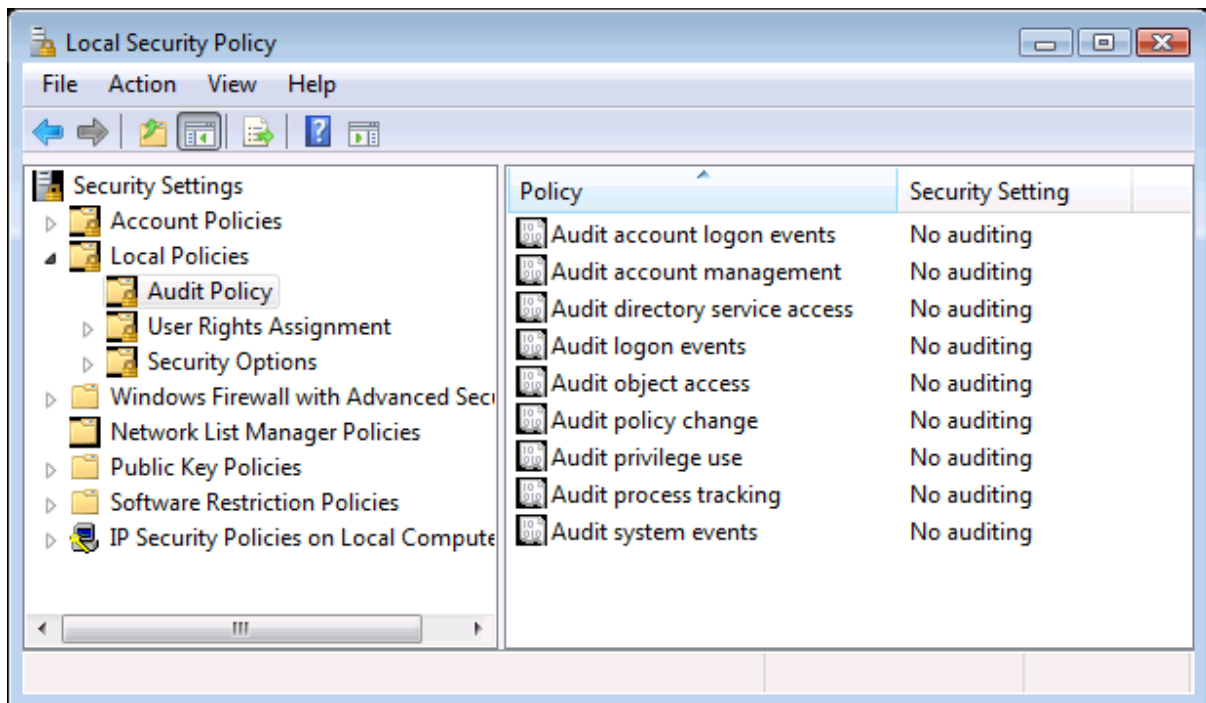
Step 1: Enable Firewall permissions

To manually enable firewall rules on Microsoft Windows Vista:

1. Click Start ► Control Panel ► Security and click Allow a program through Windows Firewall from the left panel.
2. Select **Exceptions** tab and from **Allowed programs and features** list, enable the following rules:
 - » Remote Event Log Management
 - » File and Printer Sharing
 - » Network Discovery
3. Click **Apply** to apply changes.

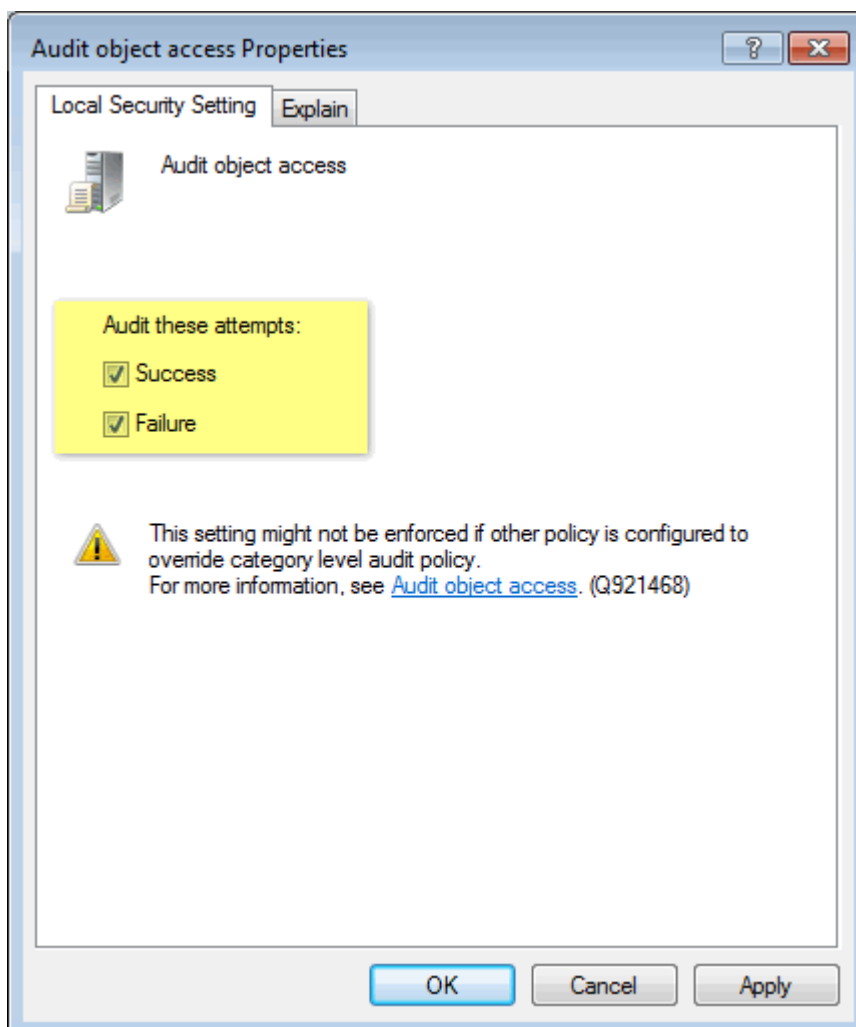
Step 2: Enable additional auditing features

1. From a command prompt key in `secpol.msc` and press **Enter**.
2. From the **Security Settings** node, expand **Local Policies** ► **Audit Policy**.



Screenshot 143 - Local security policy window

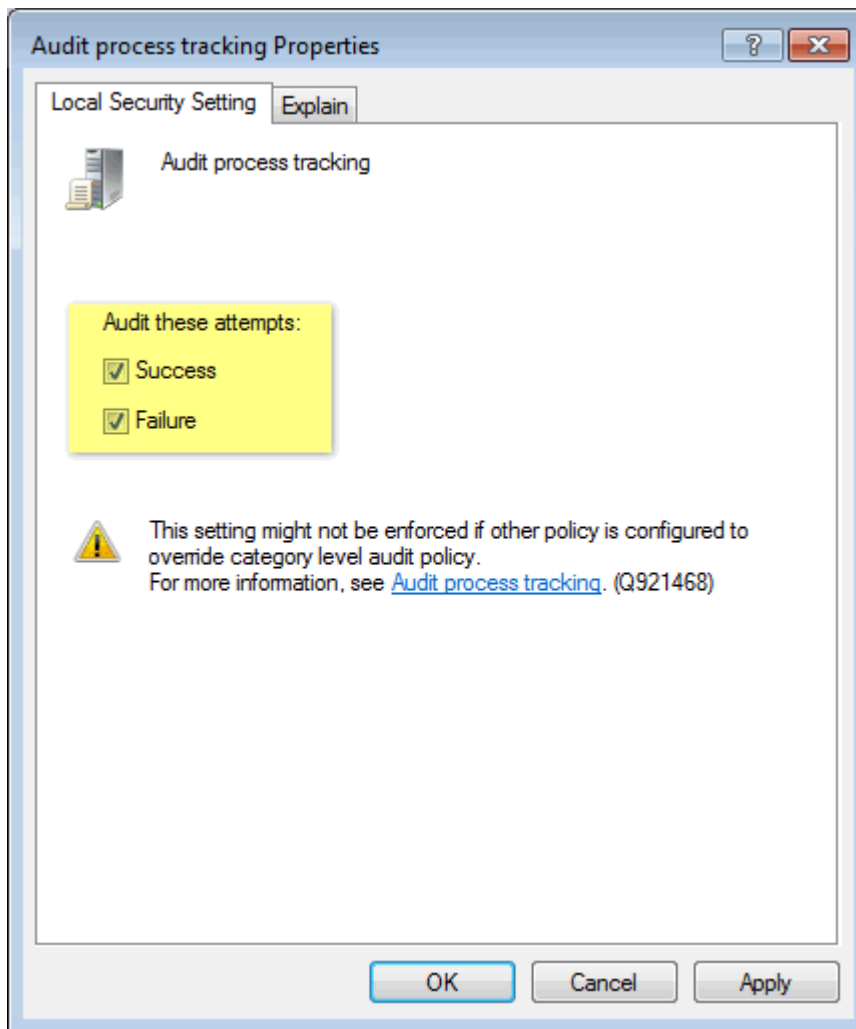
3. From the right panel, double click **Audit object access**.



Screenshot 144 - Audit object access Properties

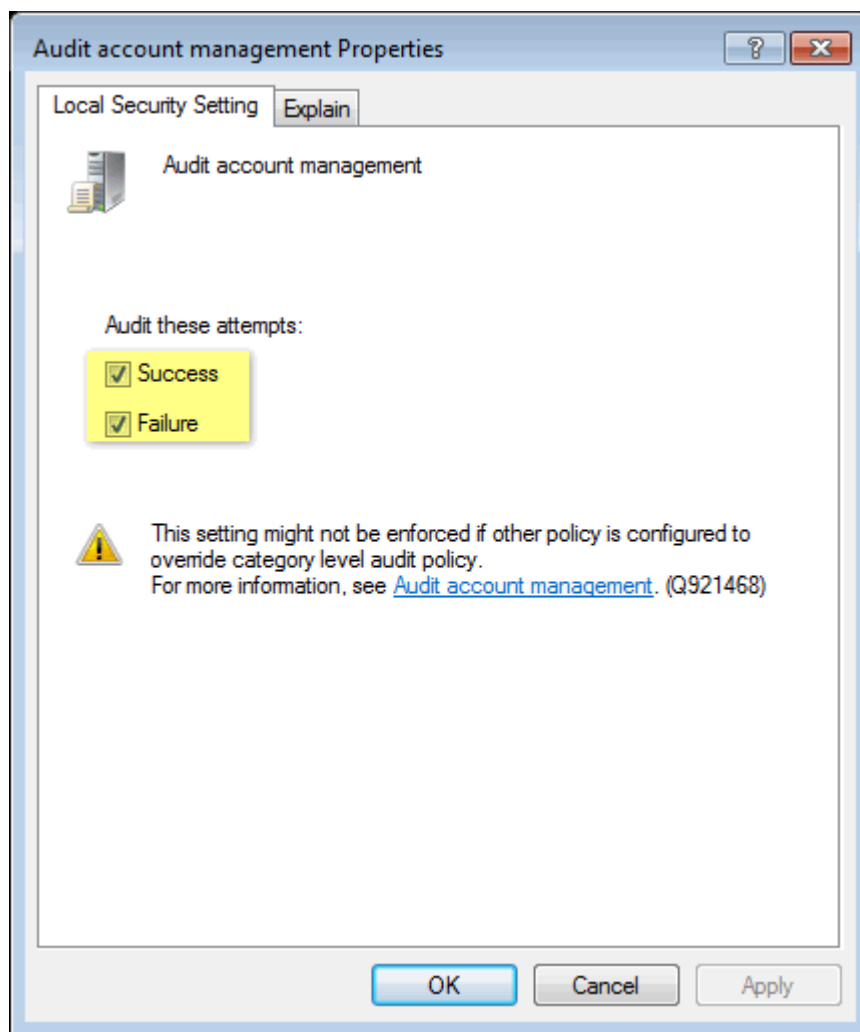
4. From the **Audit object access Properties**, select **Success** and **Failure** and click **OK**.

5. From the right panel, double click **Audit Process tracking**.



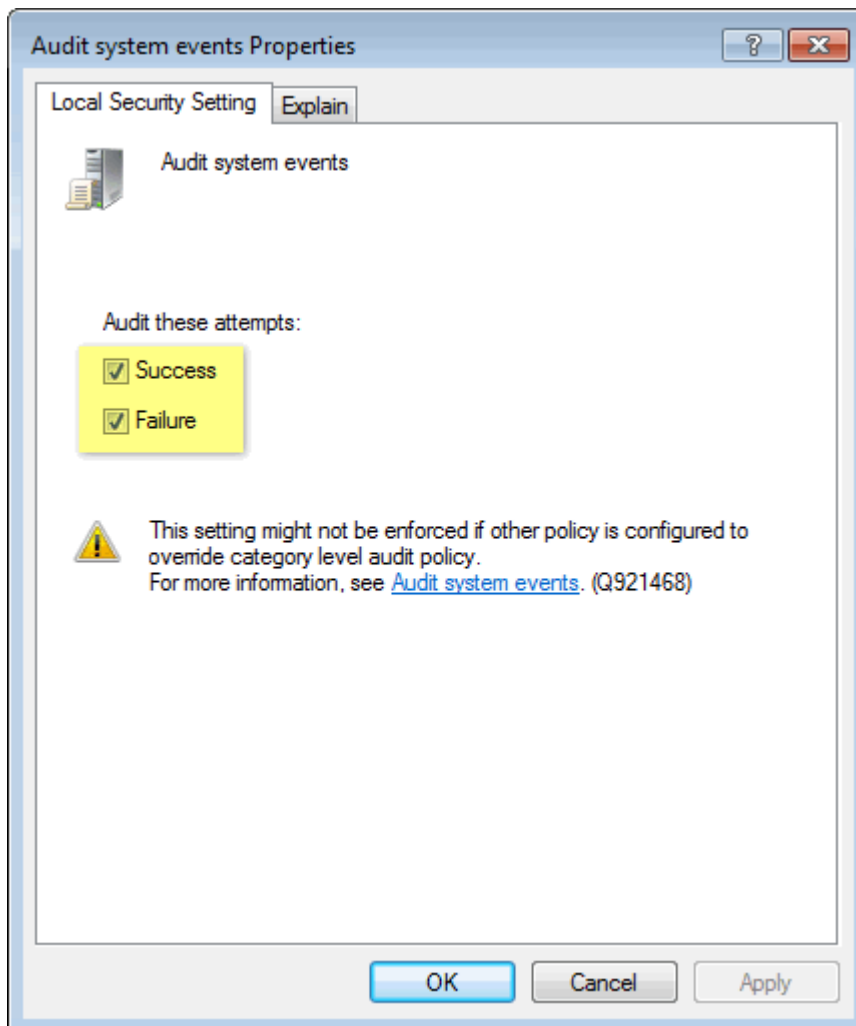
Screenshot 145 - Audit process tracking Properties

6. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.
7. From the right panel, double click **Audit account management**.
8. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.



Screenshot 146 - Audit account management properties

9. From the right panel, double-click **Audit system events**.
10. From the **Audit process tracking Properties**, select **Success** and **Failure** and click **OK**.



Screenshot 147 - Audit system events properties

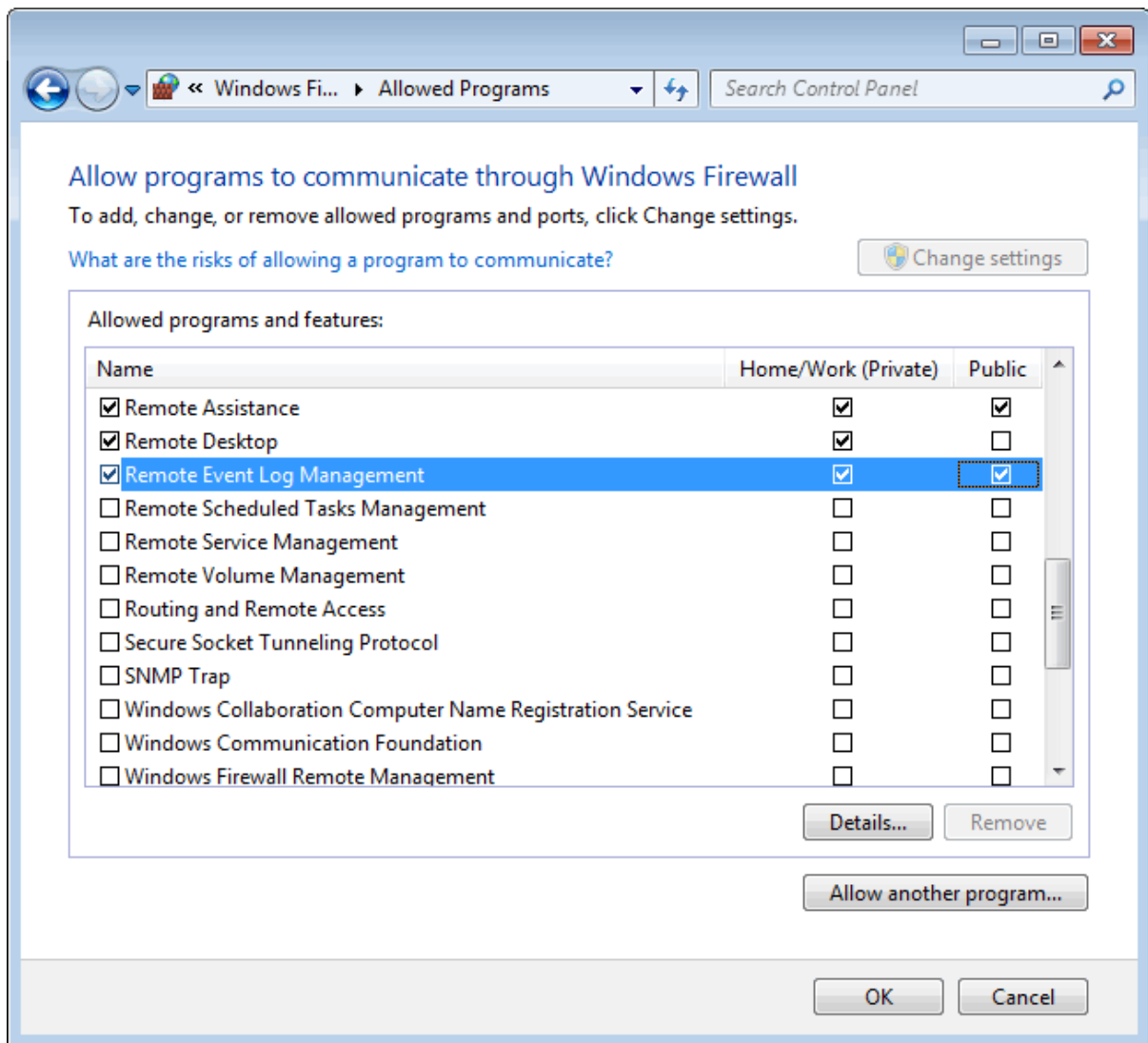
11. Close the Local Security Policy window.

13.1.3 Microsoft Windows 7

Step 1: Enable Firewall permissions

To manually enable firewall rules on Microsoft Windows 7:

1. Click **Start ► Control Panel ► System and Security** and click **Allow a program through Windows Firewall**, under **Windows Firewall** category.



Screenshot 148 - Allowed programs in Microsoft Windows Vista or later

2. From **Allowed programs and features** list, enable the following rules:

- » Remote Event Log Management
- » File and Printer Sharing
- » Network Discovery

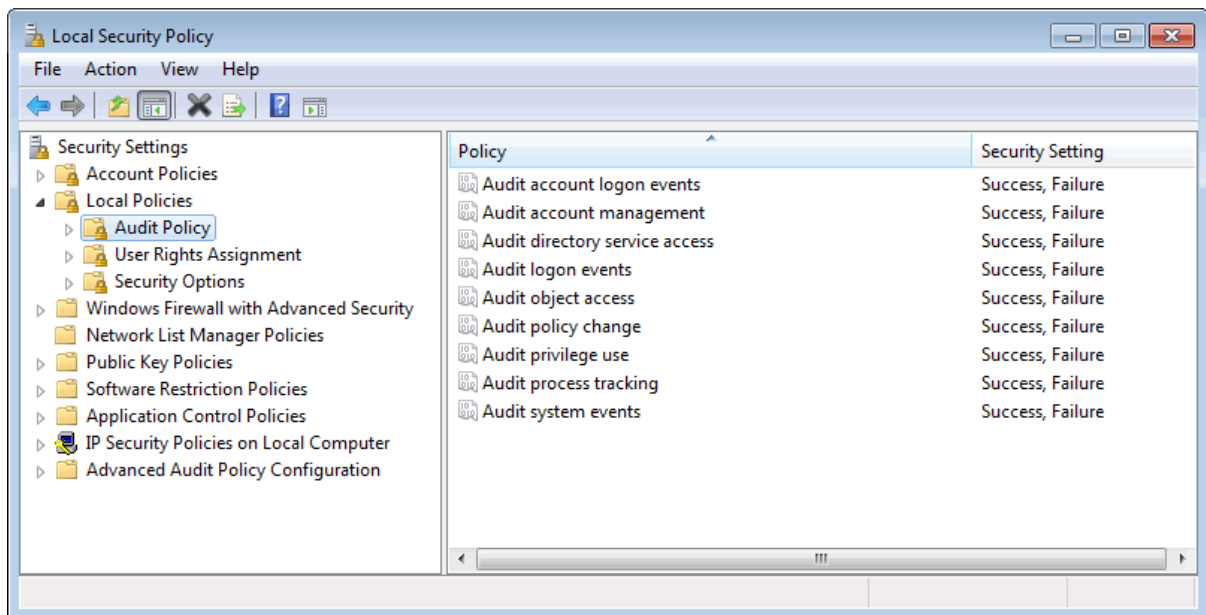
3. Select **Domain**, **Private** and **Public** for each rule mentioned above.

4. Click **OK** to apply changes.

Step 2: Enable additional auditing features

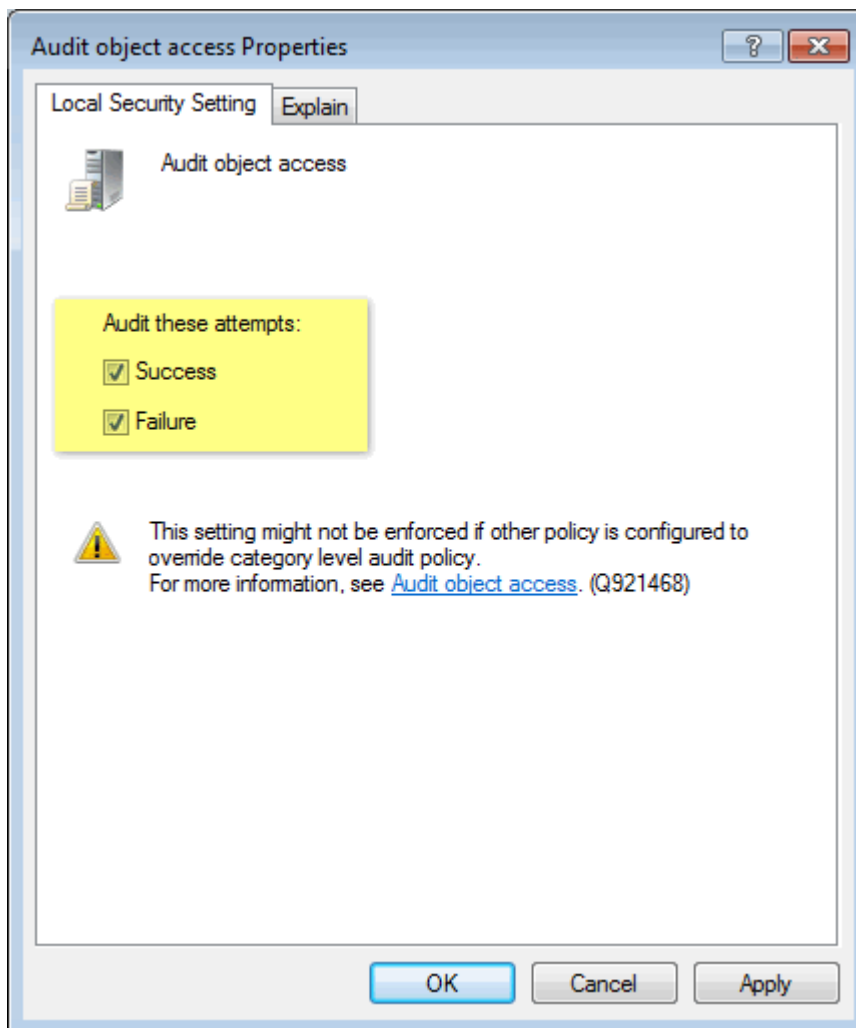
1. From command prompt key in **secpol.msc** and press **Enter**.

2. From the Security Settings node, expand Local Policies ► Audit Policy.



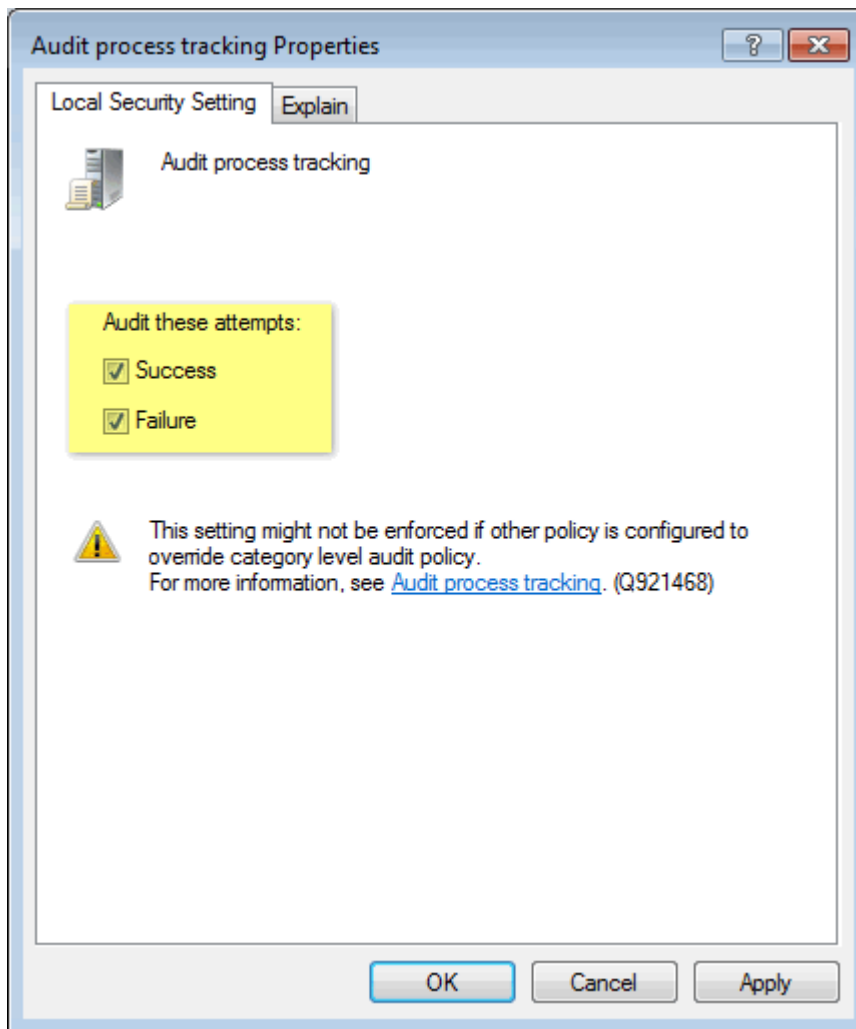
Screenshot 149 - Local security policy window

3. From the right panel, double click **Audit object access**.
4. From the Audit object access Properties, select Success and Failure and click OK.



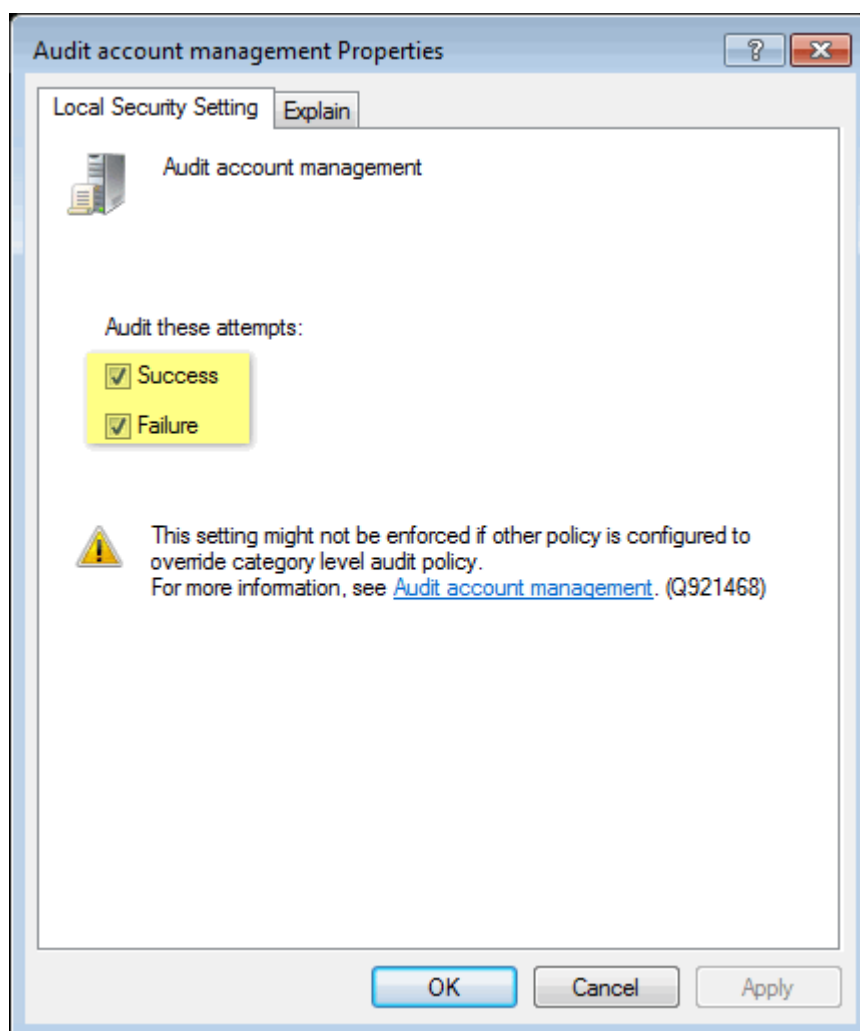
Screenshot 150 - Audit object access Properties

5. From the right pane, double click **Audit Process tracking**.
6. From the Audit process tracking Properties, select Success and Failure and click OK.



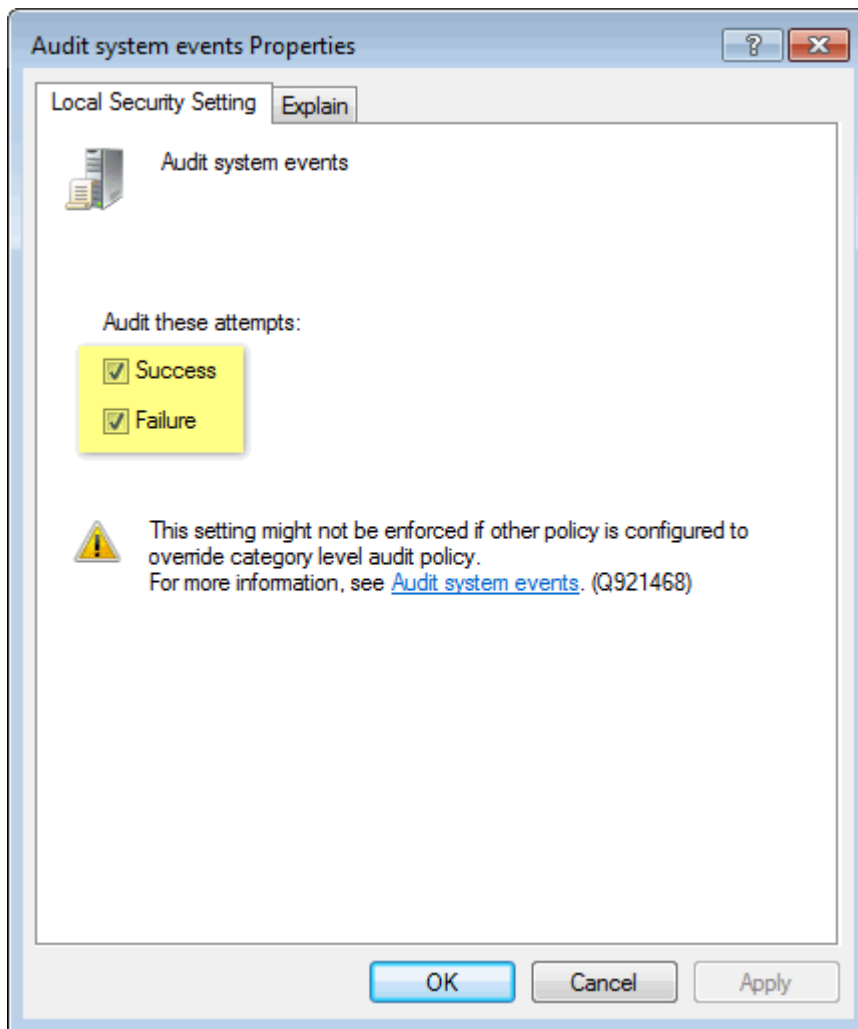
Screenshot 151 - Audit process tracking Properties

7. From the Audit process tracking Properties, select Success and Failure and click OK.
8. From the right panel, double click **Audit account management**.
9. From the Audit process tracking Properties, select Success and Failure and click OK.



Screenshot 152 - Audit account management properties

10. From the right panel, double click **Audit system events**.
11. From the Audit process tracking Properties, select Success and Failure and click OK.



Screenshot 153 - Audit system events properties

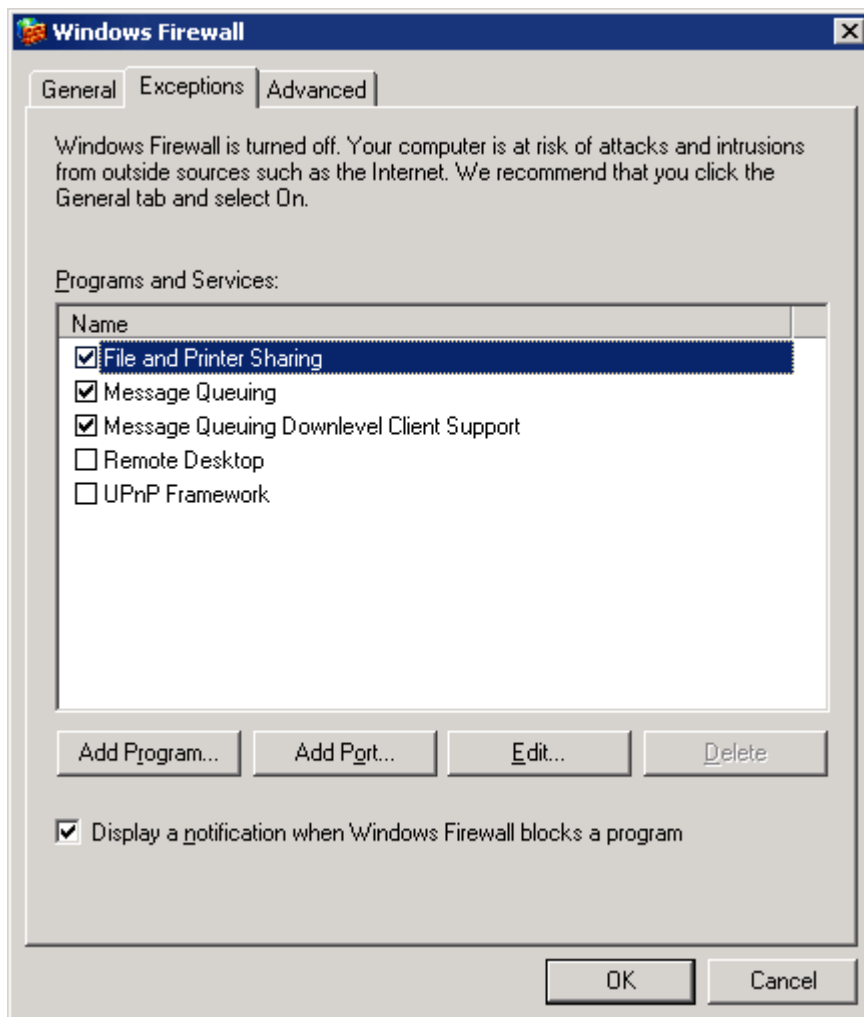
12. Close the local Security Policy window.

13.1.4 Microsoft Windows Server 2003

Enable Firewall permissions

To manually enable firewall rules on Microsoft Windows Server 2003:

1. Click **Start ► Control Panel ► Windows Firewall** and select **Exceptions** tab.



Screenshot 154 - Enable firewall rules in Microsoft Windows Server 2003

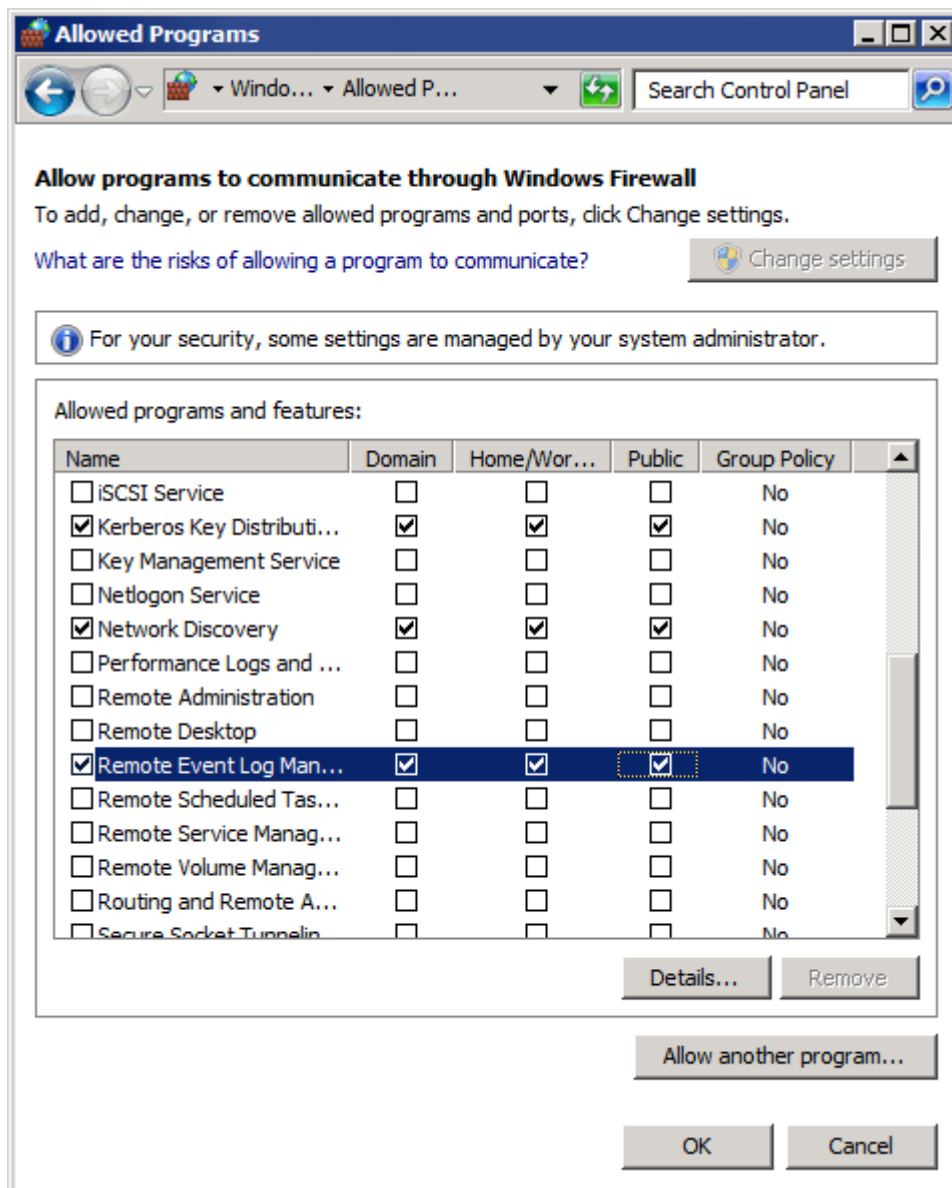
2. From **Programs and Services** list, enable **File and Printer Sharing**.
3. Click **OK** to apply changes and close.

13.1.5 Microsoft Windows Server 2008 (including R2)

Enable firewall permissions

To manually enable firewall rules on Microsoft Windows Server 2008 (including R2):

1. Click **Start ► Control Panel ► Security and Allow a program through Windows Firewall** under **Windows Firewall** category.
2. In the list of programs, enable the following:
 - » File and Printer Sharing
 - » Network Discovery
 - » Remote Event Log Management.



Screenshot 155 - Firewall rules on Microsoft Windows Server 2008

3. Click **OK** to apply changes.



In Windows Server 2008 R2, ensure to select **Domain**, **Private** and **Public** for each rule mentioned above.

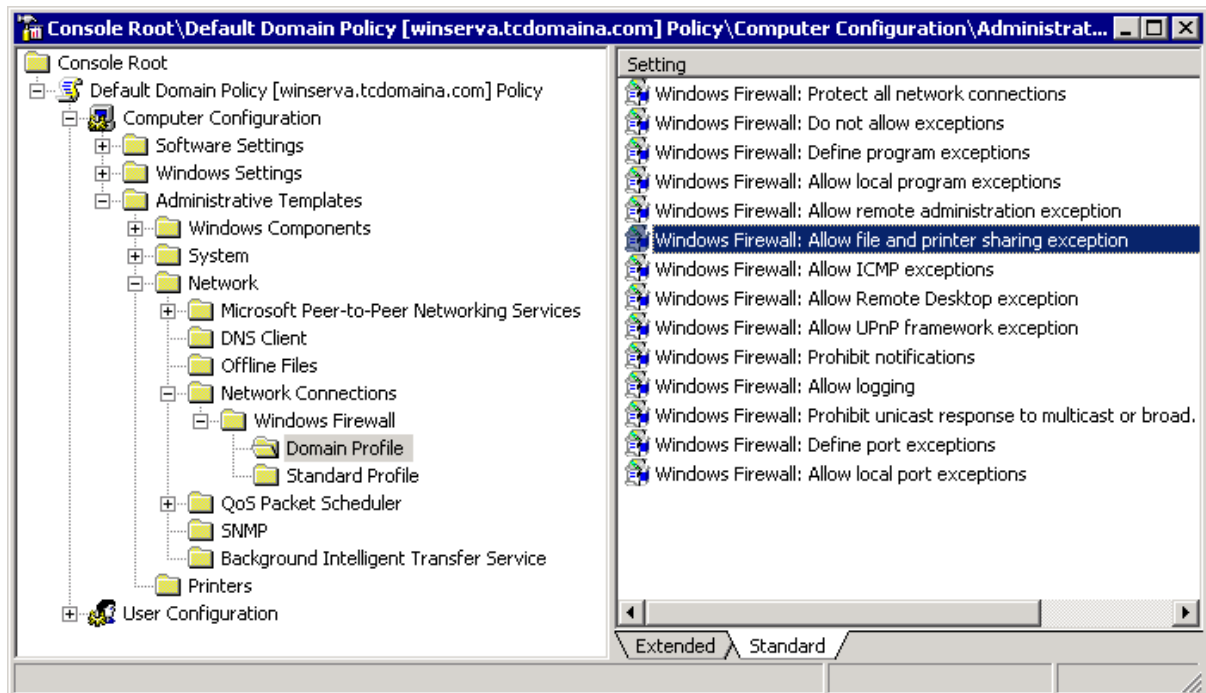
13.2 Enabling permissions on event sources automatically

13.2.1 Windows Server 2003

To open ports and enable permissions on all domain clients using Microsoft Windows Server 2003 domain controller:

1. Click **Start ► Run**, key in **mmc** and click **OK**.
2. Click **File ► Add/Remove Snap-in** and click **Add**.
3. Locate and select **Group Policy Object Editor** and click **Add**.
4. Click **Browse**, select **Default Domain Policy** and click **OK**.
5. Click **Finish**.
6. Select **Group Policy Object Editor** again and click **Add**.

7. Click Browse, double click Domain Controllers folder and select Default Domain Controllers Policy. Click OK.
8. Click **Finish** and **Close**.
9. From the Console Root, expand Default Domain Policy ► Administrative Templates ► Network ► Network Connections ► Windows Firewall ► Domain Profile.



Screenshot 156 - Domain Policy console in Microsoft Windows Server 2003

10. From the **Settings** list, right click **Windows Firewall: Allow file and printer sharing exception** and select **Properties**.
11. From the **Settings** tab, select **Enabled** and click **OK**.
12. Repeat steps 9 to 11 for Default Domain Controllers Policy.
13. Click **File** ► **Save** to save the management console.



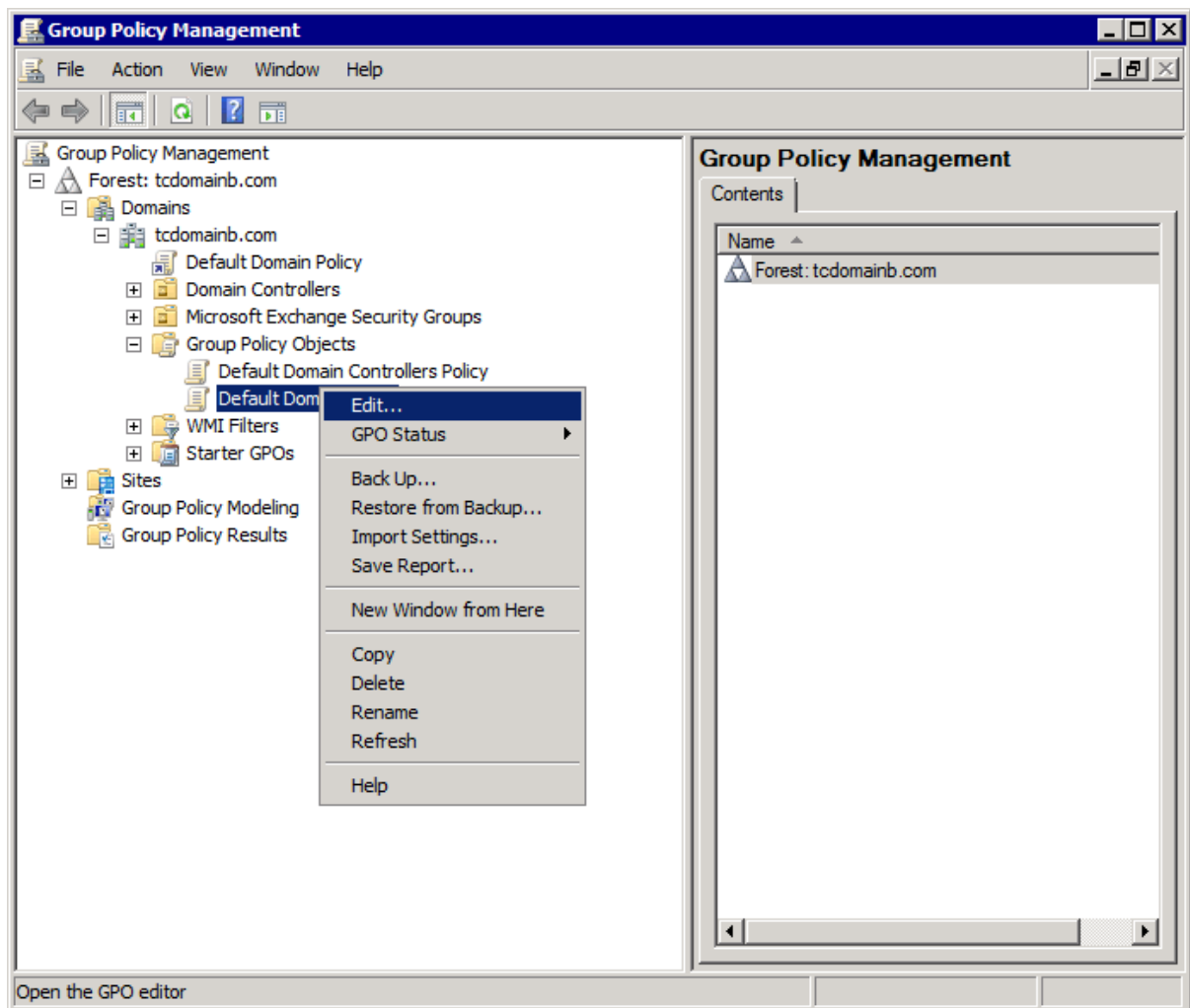
The group policy will be applied the next time each client machine is started.

13.2.2 Windows Server 2008 (including R2)

Firewall permissions

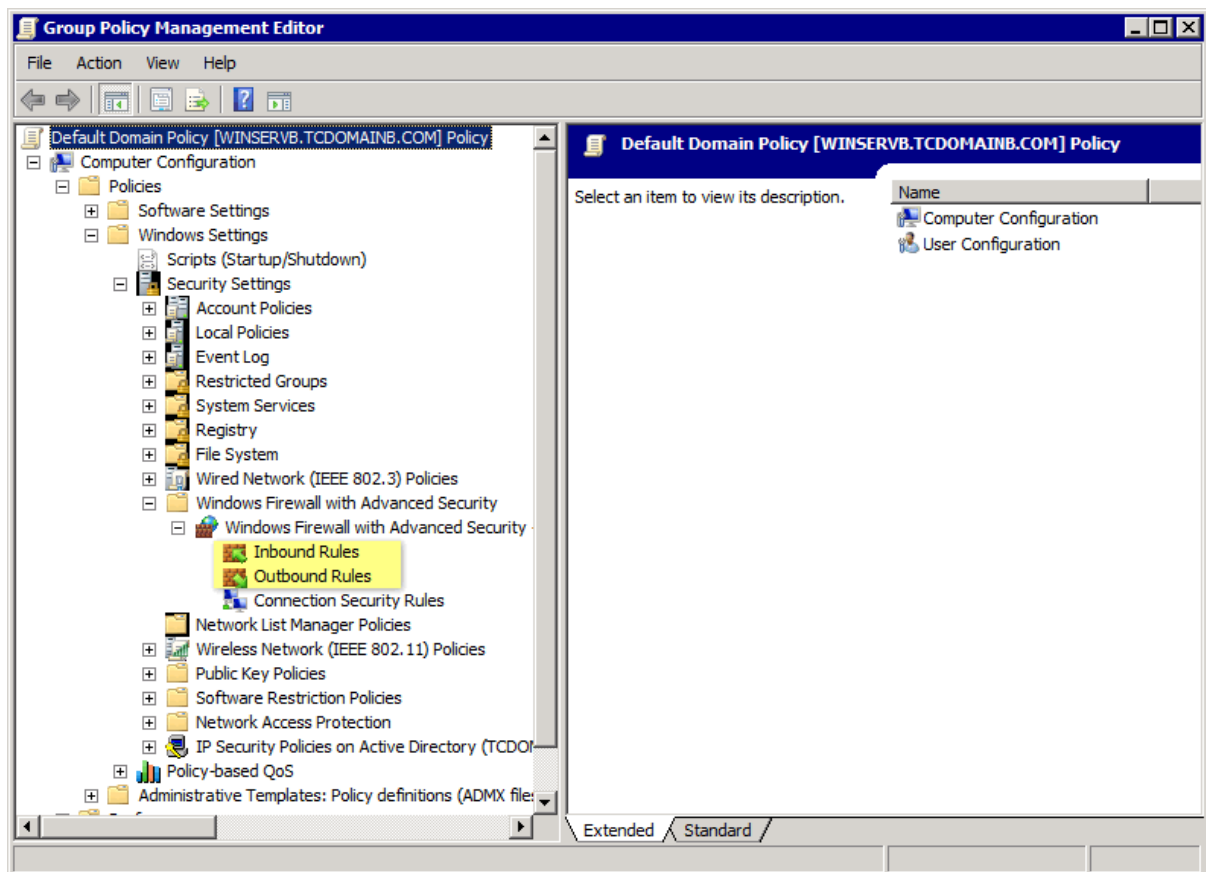
To enable permissions on all domain clients:

1. Click Start ► Administrative Tools ► Group Policy Management.
2. Expand Group Policy Management ► Forest ► Domains ► <Domain name> ► Group Policy Objects.



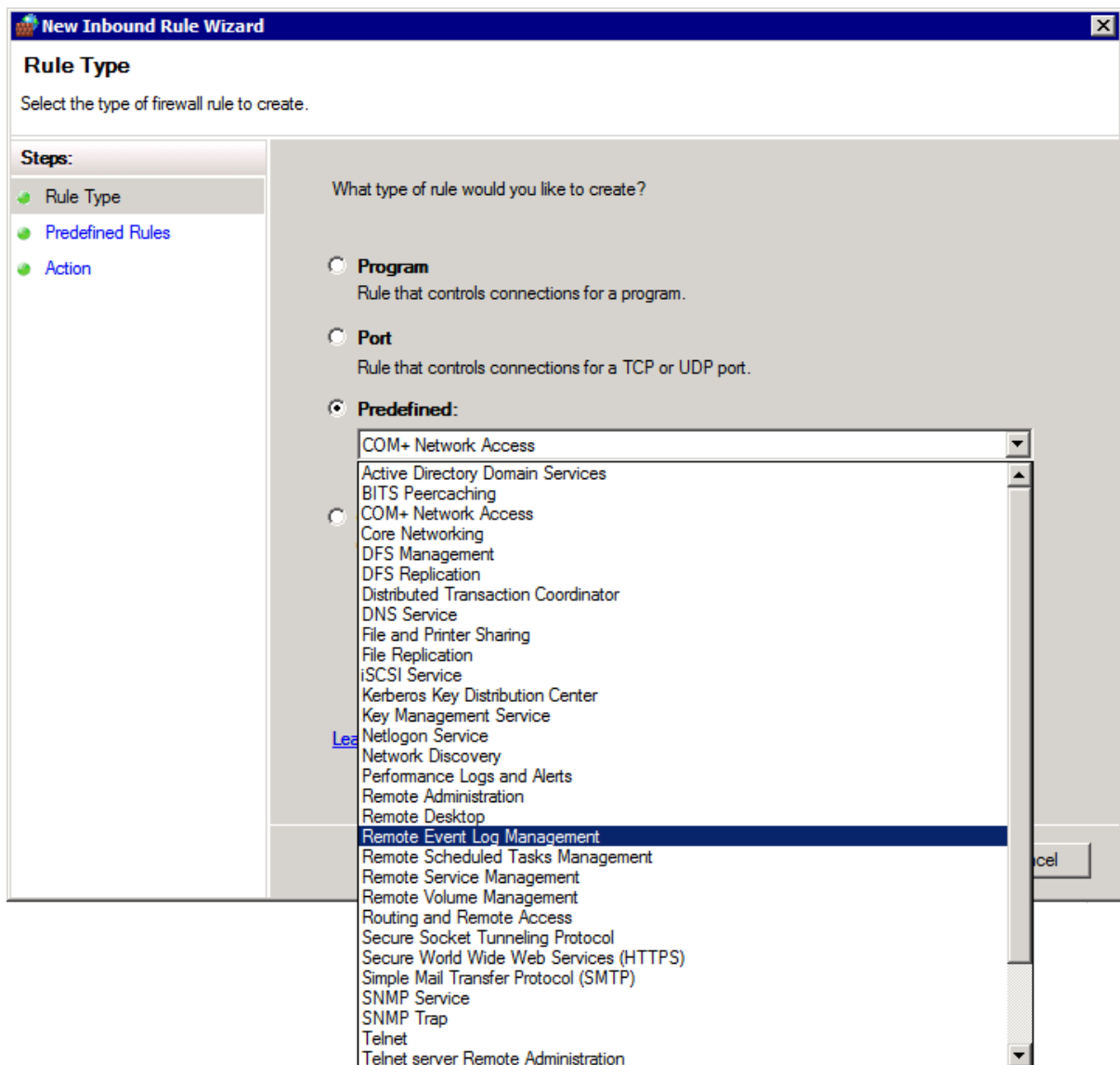
Screenshot 157 - Group Policy Management in Microsoft Windows Server 2008 R2

3. Right click **Default Domain Policy** and select **Edit**.
4. Expand **Computer Configuration** ► **Policies** ► **Windows Settings** ► **Security Settings** ► **Windows Firewall with Advanced Security**, right click **Inbound Rules** and select **New Rule...**



Screenshot 158 - Group Policy Management Editor

5. In the New Inbound Rule Wizard, select **Predefined** and select **File and Printer Sharing**.



Screenshot 159 - Predefined rules

6. Click **Next**.
7. Select all rules and click **Next**.
8. Select Allow the connection and click Finish
9. Repeat steps 5 to 8 for each of the following rules:
 - » Remote Event Log Management
 - » Network discovery
10. From Group Policy Management Editor, expand **Computer Configuration ► Policies ► Windows Settings ► Security Settings ► Windows Firewall with Advanced Security**, right click **Outbound Rules** and select **New Rule...**
11. Repeat Steps 5 to 9 while at step 9 enable only **Network Discovery**.
12. Close Group Policy Management Editor.
13. From Group Policy Management, expand Group Policy Management ► Forest ► Domains ► <Domain name> ► Default Domain Controllers Policy.
14. Repeat steps 4 to 13.
15. Close Group Policy Management.

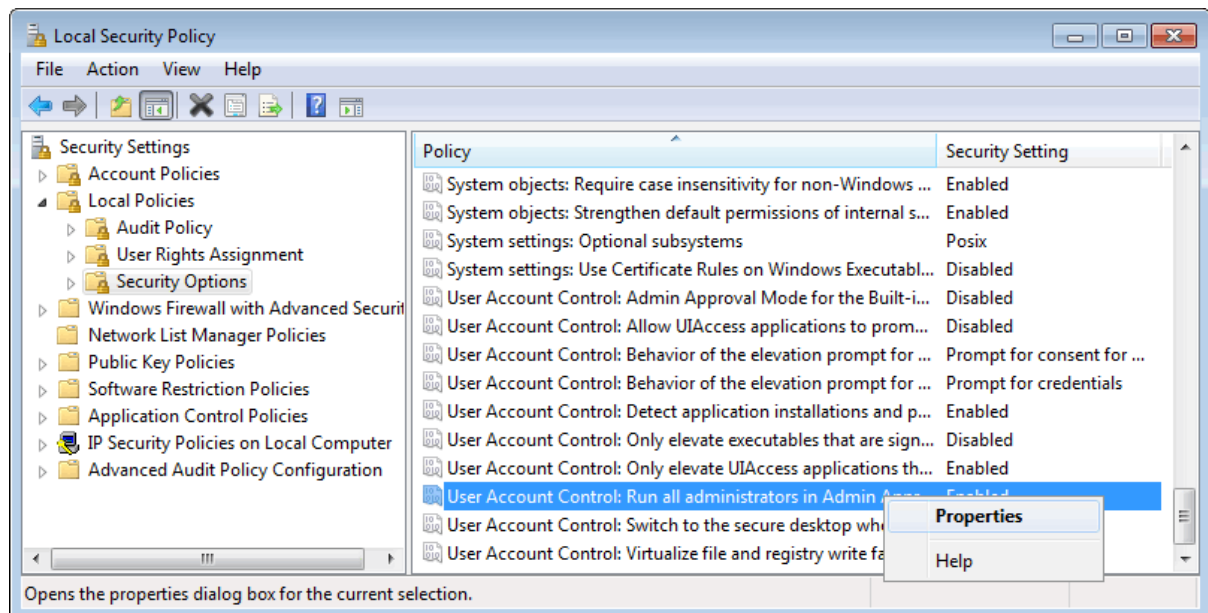


The group policy will be applied the next time each client machine is started.

13.3 Disabling UAC to scan event sources

When GFI EventsManager is configured to collect events using a local account target machines must have User Account Control (UAC) disabled. To disable UAC on Microsoft Windows Vista machines or later:

1. Click **Start ► Run**, key in **secpol.msc** and press **Enter**.
2. From the Security Settings, expand Local Policies and click Security Options.
3. Right click User Account Control: Run all administrators in Admin Approval Mode and select Properties.



Screenshot 160 - Predefined rules

4. From the **Local Security Settings** tab, select **Enabled** and click **OK**.
5. Close the **Local Security Policy** window.

13.4 Command line tools

GFI EventsManager provides you with command line tools through which you can perform various functions. These tools are located in the GFI EventsManager installation directory.

GFI EventsManager CMD tools include:

Table 83 - CMD tools

TOOL	DESCRIPTION
ESMcmdConfig.exe	<p>This CMD tool enables you to configure general settings for GFI EventsManager. Such settings include:</p> <ul style="list-style-type: none"> » GFI EventsManager logon credentials » License key » Mail server settings » Administrator email » Create/Remove Group shortcuts » Get computer names. <p>For more information, refer to Using ESMcmdConfig.exe.</p>

TOOL	DESCRIPTION
Esmdlibm.exe	Use this CMD tool to Import or Export data. For more information, refer to Using Esmdlibm.exe .
Esmreport.exe	Generates in-product reports such as configuration and job activity reports. For more information, refer to Using Esmreport.exe .
ExportHTML2PDF.exe	This CMD tool is used to export generated reports (HTML) to Portable Document Format (PDF). For more information, refer to Using ExportHTML2PDF.exe .
Importsettings.exe	Imports configuration from a data folder or from a configuration export file and is used when preserving configuration. For more information, refer to Using Importsettings.exe .
ExportSettings.exe	Exports configuration settings from GFI EventsManager installation to a configuration file. For more information, refer to Using ExportSettings.exe .
SyncComputers.exe	Use this tool to manually sync all event sources with GFI EventsManager.
Trouble.exe	Use this tool to launch GFI EventsManager troubleshooter module.
Updater.exe	Use this tool to manually check for GFI EventsManager program updates.

13.4.1 Using ESMCmdConfig.exe

To use ESMCmdConfig.exe:

1. Click **Start ► Run** and key in **CMD**.
2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.
3. Change the directory to the GFI EventsManager install directory.

CD <C:\Program Files\GFI\EventsManager 2012>

4. Key in **ESMCmdConfig.exe** followed by any of the following functions:

Table 84 - CMD: ESMCmdConfig.exe functions

FUNCTIONS	DESCRIPTION
Register Services	<p>This function registers GFI EventsManager services using an administrator account. It is made up of:</p> <ul style="list-style-type: none"> » /op:registerService - parameter name » /user:<username> - specify username » /pass:<password> - specify password. <p>Command: ESMCmdConfig.exe /op:registerService /user:Administrator /pass:1234</p>
Enable services	<p>This function enables events log management features.</p> <p>Command: ESMCmdConfig.exe /op:enable</p>
Disable services	<p>Disables GFI EventsManager and prompts the user with a custom message. It is made up of:</p> <ul style="list-style-type: none"> » /op:disable - function name » /message:<message> - specify the message to show. <p>Command: ESMCmdConfig.exe /op:disable /message:Feature is going to be disabled in one minute.</p>
Set license key	<p>This function is used to specify a license key for GFI EventsManager. It is made up of:</p> <ul style="list-style-type: none"> » /op:setLicense - function name » /licenseKey:<key> - specify the license key. <p>Command: ESMCmdConfig.exe / op:setLicense /licenseKey:XXXXXXXXXX</p>

FUNCTIONS	DESCRIPTION
Configure alerting	<p>Enable and configure alerting options. It is made up of:</p> <ul style="list-style-type: none"> » /op:configureAlerting - function name » /Server:<server> - specify server IP » /SenderEmail:<email> - specify senders' email address » /Port:<port> - specify the SMTP port (i.e. 25) » /RequiresAuthentication<true false> - specify a True or False value » /User:<username> - specify a username for the email account » /Pass:<password> - specify a password for the email account. <p>Command: ESMCmdConfig.exe /op:configureAlerting /Server:192.168.11.11 /SenderEmail:name@domain.com /Port:25 /RequiresAuthentication:True /User:Administrator /Pass:1234</p>
Set administrator's email	<p>Enables you to configure the Administrator's email. It is made up of:</p> <p>/op;setAdminEmail - function name</p> <p>/email:<email> - specify email.</p> <p>Command: ESMCmdConfig.exe /op:setAdminEmail /email:administrator@domain.com</p>
Create program group shortcuts	<p>Enables you to create group shortcuts.</p> <p>Command: ESMCmdConfig.exe /op:CreateProgramGroupShortcuts</p>
Remove program group shortcuts	<p>Enables you to remove group shortcuts.</p> <p>Command: ESMCmdConfig.exe /op:RemoveProgramGroupShortcuts</p>
Get computers	<p>Enables you to get computer names by specifying a filename where the data is exported.</p> <p>Command: ESMCmdConfig.exe /op:GetComputers /filename:ExportedNames</p>

5. Press **Enter** to run the command.

13.4.2 Using Esmplibm.exe

To use Esmplibm.exe:

1. Click **Start ► Run** and key in **CMD**.
2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.
3. Change the directory to the GFI EventsManager install directory.

CD <C:\Program Files\GFI\EventsManager 2012>

4. Key in **Esmplibm.exe** followed by any of the following functions:

Table 85 - CMD: Esmdlibm.exe functions

FUNCTIONS	DESCRIPTION
Import from SQL	<p>The Import from SQL function is used to import data from previous versions of GFI EventsManager backend database. It is made up of the following parameters:</p> <ul style="list-style-type: none"> » /importFromSql - function name » /logTypes:<application, custom, directory, security, dns, filereplication, syslog, system, snmp, oracle, sql, w3c> - specify the log types to import » /server:<serverName> - specify the SQL Server IP » /database:<maindb backupdb> - specify the database to import events from » /dbauth:<SQL WIN> - specify the authentication mode » /username:<username> - specify the SQL Server username » /password:<password> - specify the SQL Server password » /jobId:<id> - optionally, specify a unique job ID. <p>Command: Esmdlibm.exe /importFromSql /logTypes:application,w3c /server:192.168.11.11 /database:main /dbauth:SQL /username:sa /password:1234 /jobId:987</p>
Import from Dlib database	<p>This function enables you to import exported data from GFI EventsManager 2012. It is made up of the following parameters:</p> <ul style="list-style-type: none"> » /importFromDlib - function name » /path:<path> - specify the path of the import file » /name:<name> - specify the name of the import file » /anonpass1:<password> - optionally, specify the primary decryption password » /anonpass2:<password> - optionally, specify the secondary encryption password » /jobId:<id> - optionally, specify a unique job ID. <p>Command: Esmdlibm.exe /importFromDlib /path:C:\Events /name:importFile.txt /anonpass1:1234 /jobId: 987</p>
Import from Legacy File	<p>This function enables you to import data exported or archived from an older version of GFI EventsManager. It is made up of the following parameters:</p> <ul style="list-style-type: none"> » /importFromLegacyFile - function name » /path:<path> - specify the path of the import file » /logTypes:<application, custom, directory, security, dns, filereplication, syslog, system, snmp, oracle, sql, w3c> - specify the log type to import » /password:<password> - optionally, specify the password » /anonpass1:<password> - optionally, specify the primary decryption password » /anonpass2:<password> - optionally, specify the secondary encryption password » /jobId:<id> - optionally, specify a unique job ID. <p>Command: Esmdlibm.exe /importFromLegacyFile / path:C:\Events /logTypes: dns,security,w3c /password:1234 /jobId:987</p>

FUNCTIONS	DESCRIPTION
Export to file	<p>This function enables you to export data to a file. It is made up of the following parameters:</p> <ul style="list-style-type: none"> » /exportToFile - function name » /path:<path> - specify the path where the exported file is saved » /password:<password> - specify a password to protect the exported file » /olderThenXDays:<number of days> - specify what data is exported based on the number of days passed since the event was generated » /olderThenXHours:<number of hours> - specify what data is exported based on the amount of hours passed since the event was generated » /jobId:<id> - optionally, specify a unique job ID. <p>Command: Esmdlibm.exe /exportToFile /path:C:\Events /password:1234 /olderThenXDays:7 /jobId:987</p>

5. Press **Enter** to run the command.

13.4.3 Using Esmreport.exe

To use Esmreport.exe:

1. Click **Start ► Run** and key in **CMD**.
2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.
3. Change the directory to the GFI EventsManager install directory.

CD <C:\Program Files\GFI\EventsManager 2012>

4. Key in **Esmreport.exe** followed by any of the following functions:

FUNCTIONS	DESCRIPTION
Generate Configuration/Status/Events Report	<p>Enables you to generate reports based on GFI EventsManager configuration. It is made up of the following parameters:</p> <ul style="list-style-type: none"> » /type:<CONFIGURATION STATUS EVENTS> - specify report type » /target:<path> - specify destination folder » /format:<HTML CSV> - specify report format. <p>Command: Esmreport.exe /type:STATUS /target:C:\Events /format:HTML</p>
Event source configuration report	<p>Enables you to generate reports on event sources configuration. It is made up of the following parameters:</p> <ul style="list-style-type: none"> » /type:configuration - specify report type » /source:<name> - specify a single event source name <p>Or</p> <ul style="list-style-type: none"> » /group:<name> - specify a group name to report on multiple event sources. <p>Command: Esmreport.exe /type:configuration /group:Servers</p>
Status report	<p>This function is made up of the following parameters:</p> <ul style="list-style-type: none"> » /type:status - specify report type » /subtype:<MESSAGES STATS> - specify the report sub type » /period:<CURRENT "date"> - specify the period for MESSAGES sub type » /period:<"ALL TIME" date> - specify the period of STATS sub type » /options:<"ERROR MESSAGES" "ONLY WITH ISSUES"> - specify options for STATS sub type. <p>Command 1: Esmreport.exe /type:STATUS /subtype:MESSAGES /period:CURRENT</p> <p>Command 2: Esmreport.exe /type:STATUS /subtype:STATS/period:"ALLTIME" /options:"ERROR MESSAGES"</p>

FUNCTIONS	DESCRIPTION
Events report	<p>This function is made up of the following parameters:</p> <ul style="list-style-type: none"> » /type:events - specify report type » /repid:<report ID> - specify report ID » /target:<path> - specify destination folder » /format:<HTML PDF> - specify report format » /scheduled - specify report schedule. This enables schedule and uses the default settings configured in GFI EventsManager. <p>Command: Esmreport.exe /type:events /repid:11 /target:C:\Events /format:PDF</p>

5. Press **Enter** to run the command.

13.4.4 Using ExportHTML2PDF.exe

To use ExportHTML2PDF.exe:

1. Click **Start ► Run** and key in **CMD**.
2. Click **Ctrl + Shift + Enter** to run CMD with elevated privileges.
3. Change the directory to the GFI EventsManager install directory.

CD <C:\Program Files\GFI\EventsManager 2012>

4. Key in **ExportHTML2PDF.exe** followed by any of the following functions:

FUNCTIONS	DESCRIPTION
Export HTML reports to PDF	<p>This function enables you to export pre-generated HTML reports to a Portable Document Format file. It is made up of the following parameters:</p> <ul style="list-style-type: none"> » /source:<path to HTML files> - specify the source folder path which contains the HTML reports » /target:<path to PDF file> - specify the PDF destination folder. <p>Command: ExportHTML2PDF.exe /source:C:\Program Files\EventsManager 2012 /target:C:\PDFReports\EventsManager</p>

5. Press **Enter** to run the command.

13.4.5 Using ImportSettings.exe

Use this tool to import GFI EventsManager configurations previously exported.

importsettings.exe <parameters list>

PARAMETER	MANDATORY/OPTIONAL	DESCRIPTION
/operation:<operation>	Mandatory	Defines the operation to perform, either importfolder or importfile
/destination:<destination path>	Optional	Defines the destination folder where the configuration is imported
/sourceFile:<filename>	Optional	Defines the name of the file that contains the exported GFI EventsManager configuration.
/sourceFolder:<folder name/path>	Optional	Defines the name of the folder that contains the exported GFI EventsManager configuration.



Any parameter that contains spaces must be enclosed in double quotes (“”).

Example:

```
importsettings.exe /operation:importfolder: /destination:  
c:\esm\data /sourcefolder: c:\esm\old
```

13.4.6 Using ExportSettings.exe

Use this tool to export the GFI EventsManager configuration.

exportsettings.exe <parameters list>

PARAMETER	MANDATORY/OPTIONAL	DESCRIPTION
/destination:<filename>	Mandatory	Defines the file where the configuration will be exported
/folder:<folder>	Optional	To export from an alternative folder.



Any parameter that contains spaces must be enclosed in double quotes ("").

Example:

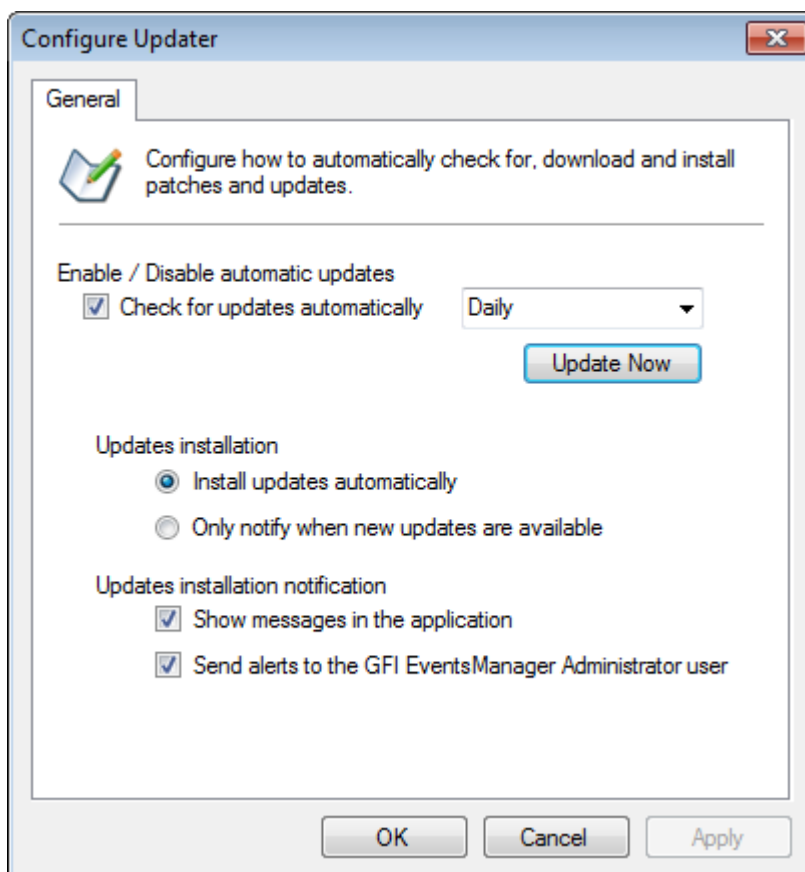
```
exportsettings.exe /destination:"c:\export"
```

13.5 Auto updating GFI EventsManager

GFI EventsManager enables users to configure how to automatically check for, download and install patches and updates.

To configure Auto Update options:

1. Launch GFI EventsManager from Start ► Program ► GFI EventsManager ► Management Console.
2. Click Edit updater options...



Screenshot 161 - Configure auto update

3. Configure the options described in Table 86 below and click **OK**:

Table 86 - Auto update options

OPTION	DESCRIPTION
Check for updates automatically	If selected, GFI EventsManager will check for updates automatically on a daily or weekly basis.
Update Now	If Check for updates automatically checkbox is not selected, use this option to manually check for updates and install missing updates.
Install updates automatically	Installs downloaded updates automatically.
Only notify me when updates are available	Available updates are shown in the Missing Updates section but are not installed.
Show messages in the application	Shows a message at the bottom of the application page. Click on the displayed message to action the updates.
Send alerts on GFI EventsManager Administrator user	Sends an email alert on the configured GFI EventsManager Administrator account. For information on configuring GFI EventsManager Administrator account refer to Configuring the Administrator account section in this manual.

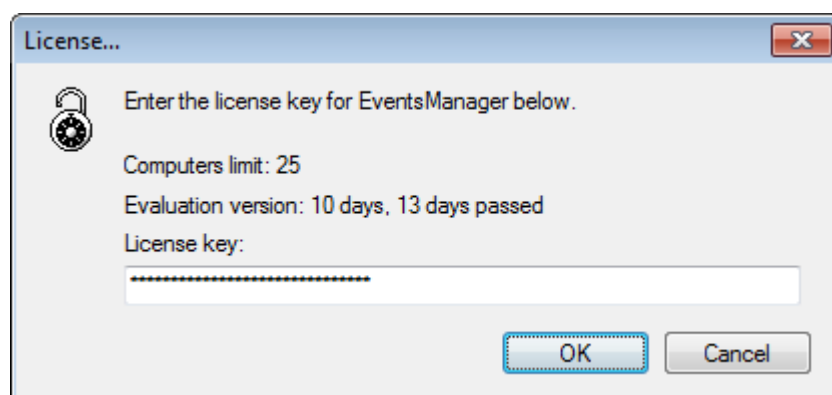
13.6 Product licensing

GFI EventsManager is licensed by Node. All devices that generate a log are considered to be a Node. This section contains information about:

- » [Updating license key](#)
- » [Obtaining a free 30-day trial license key](#)
- » [Viewing license details](#)
- » [Updating license type](#)
- » [Purchasing a license key](#)

13.6.1 Updating license key

1. Click **General** tab.
2. From the left pane, right-click **Licensing**, select **Update license key...**



Screenshot 162 - Update license key

3. Specify your license key details.
4. Click **OK** to finalize settings.

13.6.2 Obtaining a free 30-day trial license key

GFI EventsManager allows you to register your version of the product and receive a free 30-day trial. Once the trial period is expired, all event log monitoring and management services are disabled and a full license key is required.

To register and receive a 30-day trial license key:

1. Click **General** tab.
2. Click the provided link. This will take you to GFI website where you are able to enter you details and receive the license key by email.



The email address you provide in the registration form is where your free 30-day trial key will be sent. If you have a spam filtering system, make sure the email is not blocked as spam.

13.6.3 Viewing license details

1. Click **General** tab.
2. From the left pane, click **Licensing** option. Licensing details will be displayed in the right pane of the management console.
3. To view license distribution details click on **Show Details**. This will show the number of event sources configured and respective license type (such as Workstation or Server).

13.6.4 Updating license type

To change the type of license allocated to a specific event source:

1. Launch the (computer/computer group) properties dialog and click the **Licensing Type** tab.
2. By default event sources inherit their licensing type from parent group (use the license type configured in parent group properties). To change license type select the Server License or Workstation option accordingly.

13.6.5 Purchasing a license key

1. Click **General** tab.



Screenshot 163 - Buy now! Button

2. From the right pane, click **Buy now!**. This takes you to GFI website where you can view further information about licensing and purchase a valid key.



For more information about GFI EventsManager licensing, please visit:
<http://www.gfi.com/page/13789/products/gfi-eventsmanager/pricing/licensing/licensing>



For more information about GFI EventsManager pricing, please visit:
<http://www.gfi.com/products/gfi-eventsmanager/pricing>

13.7 Version information

To check your version information details:

1. Click **General** tab.
2. Click the **Version Information** option. The version information details will be displayed in the right pane.

13.7.1 Checking for newer builds

To check for newer builds of GFI EventsManager:

1. Click **General** tab.
2. From the left pane, right-click **Version Information** and select **Check for newer builds....**

14 Troubleshooting

14.1 Introduction

The troubleshooting chapter explains how you should go about resolving any software issues that you might encounter. The main sources of information available to users are:

- » The manual - most issues can be solved by reading this manual
- » GFI Knowledge Base articles
- » Web forum
- » Contacting the GFI Technical Support

This chapter contains information about:

- » Common issues
- » Knowledge Base
- » Web Forum
- » Request technical support
- » Build notifications

14.2 Common issues

ISSUE	DESCRIPTION AND SOLUTION
Error message: Not connected to the database or connection was lost.	<p>Description</p> <p>This error is encountered when GFI EventsManager is unable to connect with the SQL Database or the database connection was interrupted.</p> <p>Solution</p> <p>The following links contain information on how this issue can be solved.</p> <p>How do I debug 'Failed to connect to database'?</p> <p>http://kbase.gfi.com/showarticle.asp?id=KBID002855</p> <p>How do I configure SQL Server 2005/2008 to accept SQL Authentication?</p> <p>http://kbase.gfi.com/showarticle.asp?id=KBID002804</p> <p>How do I configure SQL Server 2000 to accept SQL Authentication?</p> <p>http://kbase.gfi.com/showarticle.asp?id=KBID002805</p> <p>Enabling TCP/IP on Microsoft SQL Server 2005</p> <p>http://kbase.gfi.com/showarticle.asp?id=KBID002920</p> <p>How to create a new database in Microsoft SQL Server</p> <p>http://kbase.gfi.com/showarticle.asp?id=KBID003379</p>
Error message: Primary Filegroup Full.	<p>Description</p> <p>This error is encountered when GFI EventsManager database backend has a maximum file size limitation and is unable to store any further data.</p> <p>Solution</p> <p>Configure the database backend to allow larger file size. This can be done on both Microsoft SQL Server and Microsoft SQL Server Express edition. For more information on how to change the maximum file size, refer to</p> <p>http://kbase.gfi.com/showarticle.asp?id=KBID003670</p>

ISSUE	DESCRIPTION AND SOLUTION
<p>Error message: Could not complete cursor operation because the table schema changed after the cursor was declared'</p>	<p>Description</p> <p>This error is encountered when the administrator is performing maintenance tasks on the GFI EventsManager databases while the GFI EventsManager service is running.</p> <p>Solution</p> <ol style="list-style-type: none"> 1. Stop GFI EventsManager service 2. Perform the maintenance tasks in Microsoft SQL server 3. Restart GFI EventsManager Service once the Microsoft SQL maintenance tasks are finished. <p>To avoid this, ensure that GFI EventsManager service is stopped whilst performing any maintenance tasks on the GFI EventsManager database.</p> <p>For more information refer to http://kbase.gfi.com/showarticle.asp?id=KBID003011</p>
<p>Error message 1:</p> <p>Error connecting to machine MACHINENAME, Error 0x35, Message: The network path was not found.</p> <p>Error message 2:</p> <p>Error connecting to machine MACHINENAME, Error 0x52E, Message: Logon failure: unknown user name or bad password.</p> <p>Error message 3:</p> <p>Critical error encountered: A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)</p> <p>Error message 4:</p> <p>Unexpected error when connecting to machine MACHINENAME; remote W3C logs path is: PATH*.*</p>	<p>Description</p> <p>These errors are encountered when GFI EventsManager tries to collect events from a machine that is not accessible over the network or the credentials are invalid.</p> <p>Possible solution 1</p> <ol style="list-style-type: none"> 1. Check that the credentials are correct 2. Check that the machine name or IP address are correct 3. Try to collect events <p>Possible solution 2</p> <p>When using a personal firewall, check that the required firewall ports are configured to allow traffic.</p> <p>For more information refer to http://kbase.gfi.com/showarticle.asp?id=KBID002770</p> <p>When using Windows firewall, check that all the required firewall permissions are enabled.</p> <p>For more information refer to http://kbase.gfi.com/showarticle.asp?id=KBID003688</p> <p>Possible solution 3</p> <p>Ensure that GFI EventsManager is installed on a supported environment. For more information on where GFI EventsManager can be installed, refer to http://kbase.gfi.com/showarticle.asp?id=KBID002842</p>
<p>No event logs are being collected by GFI EventsManager.</p>	<p>Description</p> <p>This issue can be caused by various factors and is dependent on the environment where GFI EventsManager is installed. For a checklist on how to resolve this issue, refer to http://kbase.gfi.com/showarticle.asp?id=KBID002819</p>

ISSUE	DESCRIPTION AND SOLUTION
<p>Error message 1:</p> <p>A timeout was reached (60000 milliseconds) while waiting for the GFI EventsManager service to connect.</p> <p>Error message 2:</p> <p>Error 1053: The service did not respond to the start or control request in a timely fashion.</p>	<p>Description</p> <p>The GFI EventsManager executables are digitally signed by default. When trying to start the service, the application must download the Certificate Revocation List to authenticate. If the download fails due to network connectivity or security reasons the service will fail to start by timing out.</p> <p>Possible solution 1</p> <p>Increase the default service timeout settings as described in the following Microsoft knowledgebase article</p> <p>http://support.microsoft.com/kb/941990</p> <p>Possible solution 2</p> <p>Disable Certificate revocation list (CRL).</p> <ol style="list-style-type: none"> 1. Download Microsoft Setreg application from http://ftp.gfi.com/support/setreg.zip 2. Login to the GFI EventsManager server using the GFI EventsManager service user. 3. Open command prompt 4. Change the directory to the directory storing setreg.exe 5. Run the following command: <pre>setreg.exe 3 FALSE</pre> <p>Note: The setting above can be reverted by running the following command: <code>setreg.exe 3 TRUE</code></p> <p>For more information refer to http://kbase.gfi.com/showarticle.asp?id=KBID003365</p>
<p>Error message:</p> <p>The maintenance job failed!</p>	<p>Description</p> <p>GFI EventsManager uses an ASP.Net Library called GZipStream to compress and export data from the GFI EventsManager databases. GZipStream is unable to compress data larger than 4GB. GFI EventsManager will return this error when trying to export data which is larger than 4GB.</p> <p>Solution</p> <p>In order to export the data required, use the GFI EventsManager Advanced Filters to reduce the number of Events exported. Therefore eventually reducing the size of the data which is being compressed. For more information, refer to Configuring data filter conditions section in this manual.</p>
<p>Error message:</p> <p>Event Log Records could NOT be retrieved: The RPC server is unavailable</p>	<p>Description</p> <p>This error may occur if:</p> <ul style="list-style-type: none"> The remote computer may be shut down. There may be a network hardware problem. There may be no common transports. The remote computer does not exist. A DNS entry does not exist for the remote computer in the DNS server (Try pinging the remote machine from another computer by using its host name and not its IP). <p>Investigate each possible problem and make the necessary changes. Then try to collect events from target computers.</p> <p>For more information, refer to http://kbase.gfi.com/showarticle.asp?id=KBID002820</p>

ISSUE	DESCRIPTION AND SOLUTION
<p>GFI EventsManager reports an error number 1069.</p>	<p>Description</p> <p>When installed, GFI EventsManager asks for a valid username and password. This error is encountered when an invalid password is submitted in the installation wizard.</p> <p>Solution</p> <ol style="list-style-type: none"> 1. Click Start ► Run, key in services.msc and click Ok. This will launch Services window. 2. Double Click GFI EventsManager service. 3. Select the Log On tab. 4. Ensure that the This account radio box is selected. 5. Key in a valid password for the specified User account. 6. Press OK to close the Properties window. 7. Close Services window.
<p>When collecting and processing events the CPU consumption stays constant and higher than 70%.</p>	<p>Description</p> <p>This may occur when scanning multiple domain controllers. Since domain controllers generate a large number of events and GFI EventsManager by default is configured to use a high performance level, GFI EventsManager may use a lot of CPU resources.</p> <p>Solution</p> <p>Configure GFI EventsManager to use a low performance level. To configure performance level:</p> <ol style="list-style-type: none"> 1. Select Configuration tab. 2. From the left panel, right click Performance Options and select Edit Performance options. 3. From the Performance Options dialog, select Enable GFI EventsManager service performance and select the required level. 4. Click OK. <p>Changing the performance level reduces CPU load but affect GFI EventsManager log events processing speed.</p> <p>Low performance - GFI EventsManager will Approximately process 50 events per second for each event source.</p> <p>High performance - GFI EventsManager will Approximately process from 1000 to 2000 events per second for event source.</p>

14.3 Knowledge Base

GFI maintains a Knowledge Base, which includes answers to the most common problems. If you have a problem, please consult the Knowledge Base first. The Knowledge Base always has the most up-to-date listing of technical support questions and patches. To access the Knowledge Base, visit <http://kbase.gfi.com/>.

14.4 Web Forum

User to user technical support is available via the web forum. The forum can be found at: <http://forums.gfi.com/>.

14.5 Request technical support

If you have referred to this manual and our Knowledge Base articles, and you still cannot solve issues with the software, contact the GFI Technical Support team by filling in an online support request form or by phone.

- » **Online:** Fill out the support request form on: <http://support.gfi.com/supportrequestform.asp>. Follow the instructions on this page closely to submit your support request.

- » **Phone:** To obtain the correct technical support phone number for your region please visit: <http://www.gfi.com/company/contact.htm>.



Before you contact our Technical Support team, please have your Customer ID available. Your Customer ID is the online account number that is assigned to you when you first register your license keys in our Customer Area at: <http://customers.gfi.com>.

We will answer your query within 24 hours or less, depending on your time zone.

14.6 Build notifications

We strongly suggest that you subscribe to our build notifications list. This way, you will be immediately notified about new product builds. To subscribe to our build notifications, visit:

<http://www.gfi.com/pages/productmailing.htm>.

15 Glossary

Table 87 below describes all common terms used in this manual:

Table 87 - Terms used in this manual

TERM	DEFINITION
Audit process tracking	Generates events which track actions such as programs which are launched, closed, as well as other indirect object access information which contain important security information. For more information, refer to http://technet.microsoft.com/en-us/library/cc775520(Ws.10).aspx
Actions	The activity that will be carried out as a result to events matching specific conditions. For example you can trigger actions whenever an event is classified as critical. Actions supported by GFI EventsManager include Email alerts, event archiving and execution of scripts.
Alerts	Notifications which inform recipients that a particular event has occurred. GFI EventsManager can generate Email alerts, SMS alerts and Network alerts.
Archive	A collection of events stored in the SQL Server based database backed of GFI EventsManager.
Audit account management	Generates events when account management operations are done such as create/delete a user account or group, enable/disable a user account and set/change a user password. For more information, refer to http://technet.microsoft.com/en-us/library/cc737542(Ws.10).aspx
Audit system events	Generates events when important system events happen such as user restarts or shuts down the target computer or when an event occurs that affects the security log. For more information, refer to http://technet.microsoft.com/en-us/library/cc782518(Ws.10).aspx
COM+ Network Access	Enable this firewall permission to allow client machines to access applications or services that resides on the server. This allows GFI EventsManager to access resource from all servers. For more information about this permission, refer to http://technet.microsoft.com/en-us/library/cc731967.aspx
Email alerts	Email notifications which inform recipients that a particular event has occurred. To enable email alerts, you must have access to an active mail server.
Event classification	The categorization of events as Critical, High Medium, Low or Noise.
Event logs	A collection of entries which describe events that occurred on the network or on a computer system. GFI EventsManager supports different types of event logs including: Windows Event Log, W3C Logs, Syslog, SNMP Traps and SQL Server audit events.
Event processing rules	A set of instructions which are applied against an event log.
File and Printer sharing	Enable this firewall permission to allow GFI EventsManager to access events definitions on target machines. For more information, refer to http://technet.microsoft.com/en-us/library/cc779133(Ws.10).aspx
Internet Protocol Security	A framework of open standards used to encrypt and authenticate network packets during a communication session between computers. Using cryptography services, IPsec ensures data integrity, authentication and confidentiality.
IPsec	See Internet Protocol Security

TERM	DEFINITION
Management Information Base	A MIB is the equivalent of a data dictionary or codebook. It associates object identifiers (OIDs) with a readable label and various other parameters related to an active network object such as a router. Its main function is to assemble and interpret SNMP messages transmitted from SNMP-enabled network devices. The information stored in MIBs is organized hierarchically and is normally accessible using a protocol such as SNMP.
Network alerts	Network messages (known as Netsend messages) which inform recipients that a particular event has occurred. These messages are sent through an instant messenger system/protocol and are shown as a popup in the system tray of the recipient's desktop. To setup network alerts, you must specify the name or IP of the computers where the Netsend messages will be sent.
Network discovery	Enable this firewall permission to allow GFI EventsManager to gather information about connected machines on the network that can be scanned. For more information, refer to http://technet.microsoft.com/en-us/library/cc181373.aspx
Noise	Repeated log entries which report the same event.
Object auditing	Enable this auditing feature to audit events of users accessing objects (example, files, folder and printer). For more information, refer to http://technet.microsoft.com/en-us/library/cc976403.aspx
Object auditing	Enable this auditing feature to audit tracking information (example, program activation, process exit and indirect object access). For more information, refer to http://technet.microsoft.com/en-us/library/cc775520(Ws.10).aspx
Remote Event Log Management	Required to allow GFI EventsManager to access and collect events from remote machines. For more information, refer to http://technet.microsoft.com/en-us/library/cc766438.aspx
Rule-set folder	The folder which contains one or more rule-sets.
Rule-sets	A collection of event processing rules.
SMS alerts	SMS notifications which inform recipients that a particular event has occurred. In GFI EventsManager, SMS alerts can be sent through various sources including mobile phones with modem capabilities and email-to-SMS web-based gateways.
SNMP Object Identifier (OID)	An SNMP object identifier is an address made up of a sequence of 'dotted' numbers (Example: 1.3.6.1.4.1.2682.1). These numbers uniquely identify and locate a specific device (Example: hub) within the entire network. SNMP OIDs are a key component in the assembly of SNMP messages. In fact, an SNMP server cannot interpret or assemble messages which don't have an OID. Individual vendors often create their own MIBs that only include the OIDs associated specifically with their device.
SNMP Traps	Notifications/alerts generated and transmitted by active network components (Example: hubs, routers and bridges) to SNMP server(s) whenever important events such as faults or security violations occur. Data contained in SNMP Traps may contain configuration, status as well as statistical information such as number of device failures to date.
Syslog messages	Notifications/alerts most commonly generated and transmitted to a Syslog server by UNIX and Linux-based systems whenever important events occur. Syslog messages can be generated by workstations, servers as well as active network devices and appliances such as Cisco routers and Cisco PIX firewalls to record failures and security violations amongst other activities.
Unclassified events	Events that did not satisfy any of the event processing conditions configured in the event processing rules.

TERM	DEFINITION
W3C logs	W3C is a common log format developed by the World Wide Web Consortium. W3C logs are text-based flat files used mainly by web servers including Microsoft Internet Information Server (IIS) to record web related events such as web logs.
Windows Event Logs	A collection of entries which describe events that occurred on a computer system running Windows OS.

A

Account Usage Reports 37

anti-virus 17

Archiving events 73, 79

D

Daily Digest 1, 52, 53

Database Backend 1, 2, 3, 4, 7, 8, 16, 73, 75, 79, 81, 103, 137, 141, 185

Database Operations 5, 141, 142, 145, 147, 149, 152, 153, 155, 157

Demilitarized Zone 13, 14

DNS server 9, 14, 91, 92, 187

E

Email Alerts 89, 114, 191

Event classification 4, 90, 114, 116, 191

Event color-coding 1, 3, 4, 27, 31

Event finder tool 1, 3, 4, 27, 32

Event processing rules 1, 3, 4, 7, 70, 86, 87, 89, 90, 105, 106, 136, 191, 192

Event query 3, 4

Events Browser 1, 3, 8, 28, 31, 32, 111, 142

EventsManagerAdministrator 123, 127

Export events to CSV 33

F

firewall 17

G

GFI EndPointSecurity 61, 86, 87

GFI LANguard 61, 85, 86, 136

I

Installation wizard 188

L

License type 61, 182, 183

Licensing 2, 8, 18, 62, 158, 182, 183

GFI EventsManager

Logon credentials 62, 67, 68, 72, 76, 79, 82

M

Management Information Base 5, 99, 192

N

Network alerts 7, 105, 124, 191, 192

Noise Reduction 4

O

Operational time 62, 68, 69, 72, 79, 109

Oracle database 3, 61, 77, 78, 79, 80, 81, 82, 83, 84

P

Performance Options 188

Q

Quick Start Dialog 21, 22, 24

R

Rule-set 1, 89, 90, 105, 106, 107, 192

S

SMS alerts 191, 192

SNMP traps 3, 7, 9, 11, 16, 62, 65, 71, 89, 98, 99, 100, 101, 137, 138, 139, 191, 192

SQL Server audit 5, 9, 11, 13, 73, 89, 191

Storage Folder 7, 73, 103, 141

Syslog messages 7, 10, 13, 15, 16, 95, 97, 98, 192

Syslog server 10, 15, 95, 97, 98, 192

V

version information 158, 183, 184

W

W3C logs 3, 7, 9, 10, 62, 71, 89, 93, 94, 112, 186, 191, 193

WAN Connector 5

Windows 7 15, 16, 17, 158, 163

Windows Event Logs 3, 4, 7, 9, 62, 89, 92, 93, 102, 106, 193

Windows Vista 15, 16, 17, 28, 92, 137, 158,
159, 164, 175

USA, CANADA, CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

Email: ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

Email: sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

Email: sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

Email: sales@gfiap.com



© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided “as is” with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out- of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.